Sponsored by the Office of Naval Research (ONR)

ONR Decision-Support Workshop Series

Developing the New Infostructure

hosted by the

Collaborative Agent Design Research Center (CADRC)
Cal Poly State University, San Luis Obispo, CA

Proceedings of Workshop held on September 10-11, 2003

at
The Clubs at Quantico, Quantico Marine Corps Base
Quantico, VA

December 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Developing the New Infostructure - Annual ONR Workshop on Collaborative Decision-Support Systems held on September 10-11, 2003	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Collaborative Agent Design Research Center (CADRC) Cal Poly State University, San Luis Obispo, CA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001754.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**310**	

Preamble

In August of 1998 the Collaborative Agent Design Research Center (CADRC) of the California Polytechnic State University in San Luis Obispo (Cal Poly), approached Dr. Phillip Abraham of the Office of Naval Research (ONR) with the proposal for an annual workshop focusing on emerging concepts in decision-support systems for military applications. The proposal was considered timely by the ONR Logistics Program Office for at least two reasons. First, rapid advances in information systems technology over the past decade had produced distributed, collaborative computer-assistance capabilities with profound potential for providing meaningful support to military decision makers. Indeed, some systems based on these new capabilities such as the Integrated Marine Multi-Agent Command and Control System (IMMACCS) and the Integrated Computerized Deployment System (ICODES) had already reached the field testing and final product stages, respectively.

Second, over the past two decades the US Navy and Marine Corps have been increasingly challenged by missions demanding the rapid deployment of forces into hostile or devastated territories with minimum or non-existent indigenous support capabilities. Under these conditions Marine Corps forces have to rely mostly, if not entirely, on sea-based support and sustainment operations. Operational strategies such as Operational Maneuver From The Sea (OMFTS) and Sea To Objective Maneuver (STOM) are very much in need of intelligent, real-time and adaptive decision-support tools to assist military commanders and their staff under conditions of rapid change and overwhelming data loads. In the light of these developments the Logistics Program Office of ONR considered it timely to provide an annual forum for the interchange of ideas, needs and concepts that would address the decision-support requirements and opportunities in combined Navy and Marine Corps sea-based warfare and humanitarian relief operations.

The first ONR Workshop (***Collaborative Decision Making Tools***) was held April 20-22, 1999 and focused on advances in technology with particular emphasis on an emerging family of powerful computer-based tools. The workshop concluded that the most able members of this family of tools appear to be computer-based agents that are capable of communicating within a virtual environment of objects and relationships representing the real world of sea-based operations. Keynote speakers included: VAdm Jerry Tuttle (USN Ret.); LtGen Paul Van Riper (USMC Ret.); RAdm Leland Kollmorgen (USN Ret.); and, Dr. Gary Klein (Chairman, Klein Assoc.).

The second ONR Workshop (***The Human-Computer Partnership in Decision-Support***) held May 2-4, 2000, was structured in two parts: a relatively small number of selected formal presentations (i.e., technical papers) followed each afternoon by four concurrent open forum discussion seminars. Keynote speakers included: Dr. Ronald DeMarco (Assoc. Technical Director, ONR); RAdm Charles Munns (USN); Col Robert Schmidle (USMC); and, Col Ray Cole (USMC Ret., Program Manager ELB ACTD, ONR).

The third ONR Workshop (***Continuing the Revolution in Military Affairs***) was held June 5-7, 2001 and focused on: the changing role of the military in a post Cold War environment; adaptive interoperable decision-support systems utilizing intelligent collaborating software agents; and, the transitional period. Keynote speakers included Mr. Andrew Marshall, Head of the Pentagon's Office of Net Assessment, and RAdm Jay M. Cohen, Chief of Naval Research, Office of Naval Research (ONR).

The fourth ONR Workshop (***Transformation ...***) was held on September 18-19, 2002 at The Clubs in Quantico on the Quantico Marine Corps Base, Quantico, Virginia. Keynote speakers included VAdm Jerry Tuttle (USN Ret.) and Steven Cooper (Special Assistant to the President, Senior Director for Information Integration and CIO, Office of Homeland Security).

The fifth ONR Workshop (***Developing the New Infostructure***) described in these proceedings was held on September 10-11, 2003, at The Clubs in Quantico on the Quantico Marine Corps Base, Quantico, Virginia.

Copies of the proceedings of past Workshops are available free of charge from: CAD Research Center, Cal Poly (Bdg. 117 T), San Luis Obispo, CA 93407

Table of Contents

Preamble iii

Table of Contents v

Opening Remarks and Foreword vii

Workshop Program xi

About the Speakers xv

Keynote Address: Taking Power to the Edge: the Use of Agent Technology in Decision Support **1**
Richard P. (Dick) Lee, Assistant Deputy Under Secretary (Interoperability and Network Centric Warfare) Office of the Secretary of Defense

Achieving the Joint Vision: The Role of Operational Context in Future Systems **11**
Erik Chaum, U.S. Naval Undersea Warfare Center Division Newport, Newport, Rhode Island

Software Agents to Reason About Situational Awareness **29**
Dr. Mark Youngren, the MITRE Corporation, McLean, Virginia

Ontology-Based Applications for Automating Decision Support **41**
Dr. Francisco Loaiza and Dr. Steven Wartik, Institute for Defense Analyses, Alexandria, Virginia

A Web-Centric Collaborative Decision Tool and Ontology Based on Subjective Sampling and Assessing Decision Times Among Options **55**
Dr. Jerald L. Feinstein, The George Washington University, Washington, DC

Demonstration of a Typical Ontology-Based Collaborative Agents System: SEAWAY **69**
Col. Tony Wood (USMC Ret.) and Dr. Jens Pohl, Collaborative Agent Design Research Center, Cal Poly, San Luis Obispo, California

Countering Threats to America's Public Telephone Networks **79***
Dr. Sujeet Shenoi, University of Tulsa, Tulsa, Oklahoma

Internet-Telephone Network Convergence: Themes and Security Issues **81***
Dr. Anthony Meehan, University of Tulsa, Tulsa, Oklahoma

Multi-Agent Modeling of the Urban Operational Environment **83**
Dr. Frederick J. Diedrich, Aptima, Inc., Woburn, Massachusetts

ARES Agent Technology Overview **91**
Adam Gray, CDM Technologies, Inc., San Luis Obispo, California

* Due to the sensitive nature of the material covered by Dr. Sujeet Shenoi and Dr. Anthony Meehan, we are unable to include their presentations in these proceedings.

Ontological Approaches for Semantic Interoperability **101**
Michael Zang, CDM Technologies, Inc., San Luis Obispo, California

The Development of Complex Adaptive System Based Decision Support Systems **111**
Dr. John Hummel, Argonne National Laboratory, Argonne, Illinois

Keynote Address: Information in the Execution of the Homeland Security Mission **121**
(Mr. O'Neil graciously substituted for Dr. Maehl at short notice.)
Mr. Michael O'Neil, Homeland Security and Services Division, Integrated Defense Systems, The Boeing Company, Seal Beach, California

A Paradigm Shift for Information Technology **145**
Robert Kidwell, Vice President, ManTech Advanced Systems International, Inc., Fairmont, West Virginia

Leveraging a Global and Adaptable Infrastructure **165**
Mr. Mark Adams, Chief Technical Officer, Iridium Satellite LLC, Leesburg, Virginia

Wireless Sensor Networks - Technology for Detection and Protection **173**
Mike Horton, Founder and CEO, Crossbow Technology, Inc., San Jose, California

Evolving Systems to Support the Global Information Grid **189**
Dr. Thomas McVittie, Jet Propulsion Laboratory/Caltech, Pasadena, California

SecureOrigins: National Strength Through Security and Competitiveness **207**
Hector Holguin, e-plaza, Holguin Group, El Paso, Texas

A Data Strategy for the 'Virtual Border': Repurposing Commercial Information for Homeland Security Risk Assessment **225**
Robert Quartel, Chairman and CEO, and Eric Chasin, CTO, FreightDesk Technologies, Dunn Loring, Virginia

A Regional Supply Chain Simulation Model using Artificial Intelligence **233**
Dr. Larry Mallon, Director, CITT, Long Beach State University, California

Understanding Operational Collaboration in the Fleet **261**
Dr. Sunoy Banerjee, Center for Naval Analyses, Alexandria, Virginia

Understanding and Applying the Cognitive Foundation of Effective Collaboration **269**
Dr. David Noble, Evidence Based Research, Inc., Vienna, Virginia

Opening Remarks

as a Foreword to the 5th Annual Office of Naval Research (ONR) Workshop

Good Morning ! I would like to welcome you to this fifth annual Collaborative Decision-Support Workshop sponsored by the *Littoral Combat/Power Projection FNC (Full Naval Capability) Program in the Office of Naval Research (ONR)*. I am Jens Pohl, Executive Director of the Collaborative Agent Design Research Center (CADRC) at Cal Poly State University in San Luis Obispo, California.

Our Center and Cal Poly has had the honor of hosting this Workshop since 1999, and I thank you for your attendance this year. We are greatly encouraged by the steadily increasing attendance each year, to the point that we have standing room only this year with over 230 registrations. I believe that we have been able to assemble an excellent program of speakers who will share their expert knowledge and insights with us over the next two days.

Let me say a few words about the purpose of these Workshops. First and foremost, these Workshops are intended to bring together representatives from three communities that have an important stake in information technology (IT):

- The military and civilian users, who use IT as a critical decision-making capability.
- The government agencies that support the development and integration of IT.
- And of course industry, which actually develops most of the IT products.

Second, these Workshops should identify developing trends, technical limitations that require urgent attention, and opportunities for innovation. In other words, the attendees of each Workshop should go away with a better understanding of the current state of IT, where IT is likely to be headed over the next three years, and how these emerging IT capabilities can be harnessed in support of military needs and objectives.

Third, the attendees (i.e., representatives of the three communities) should have opportunities for sharing ideas and concerns on a one-to-one, informal basis throughout the duration of the Workshop. The facilities here at The Clubs at Quantico are particularly well suited for such informal interactions. And, this is also why we have catered for and integrated the morning, lunch and afternoon breaks into the Workshop program itself. In other words, we consider them to be an important part of the program.

I would like to thank *Mr. Barry Blumenthal, Program Manager of the Littoral Combat/Power Projection FNC in the Office of Naval Research (ONR)*, who sponsored this year's Conference, and at the same time recognize *Dr. Phillip Abraham* who established this *Annual ONR Workshop Series* in 1999.

The theme of this year's Workshop is "***Developing the New Infostructure***". The new Infostructure is a vision of enormous scope. However, it is also a most exciting proposition. The Global Information Grid (GIG) is the vision that will guide the Department of Defense (DoD) in the implementation of an integrated network of knowledge management services and capabilities. Succinctly stated the GIG is envisioned as a net-centric environment of seamlessly interconnected data sources and utilization capabilities. This includes "… the globally

interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policymakers, and support personnel." (John Stenbit, *The DoD Net-Centric Data Strategy*, May 2003 (Page 1). The implementation of this vision will require: (1) the standardization of nomenclature and reference tables; (2) the definition of logical data models; (3) the publication of data encoding protocols and formats (i.e., metadata registries); (4) the adoption of data transmission standards; (5) the development of functionally created ontologies that allow data to be placed in context; (6) the publication of business rules and the encoding of these rules in software agents with automated reasoning capabilities; and (7) the formulation of policies, conventions, and processes, designed to facilitate planning, problem solving, and decision-making tasks.

All of these requirements are driven by the increasing need to automate at least the lower level data interpretation tasks that have been the almost exclusive province of the human users of computer systems. This has become necessary for several reasons. First, the increased ability to collect and store data in computers has created a bottleneck. The need to interpret the vast amounts of data has simply exceeded the availability of human resources. Second, human resources are desperately needed for higher-level information analysis to counteract increasing threats from adversaries. Currently, most of the available human resources are fully employed at the lower levels of data interpretation. Third, there is an increasing need for more rapid and accurate decision-making capabilities. Typically, commanders and their staff find themselves in continuous replanning mode as the most carefully laid plans require significant adjustments due to unforeseen events that will inevitably occur during implementation.

The larger an organization the more data it generates itself and captures from external sources. With the availability of powerful computer hardware and database management systems the ability of organizations to store and order these data in some purposeful manner has dramatically increased. However, at the same time, the expectations and need to utilize the stored data in monitoring, planning and time-critical decision-making tasks have become a major human resource intensive preoccupation. In many respects this data-centric focus has become a bottleneck that inhibits the ability of the organization to efficiently and effectively accomplish its mission.

The reasons for this bottleneck are twofold. First, large organizations are forced to focus their attention and efforts on the almost overwhelming tasks involved in converting unordered data into purposefully ordered data (Figure 1). This involves, in particular, the establishment of gateways to a large number of heterogeneous data sources, the validation and integration of these sources, the standardization of nomenclatures, and the collection of data elements into logical data models.

Second, with the almost exclusive emphasis on the slicing and dicing of data, rather than the capture and preservation of relationships, the interpretation of the massive and continuously increasing volume of data is left to the users of the data (Figure 2). The experience and knowledge stored in the human cognitive system serves as the necessary context for the interpretation and utilization of the ordered data in monitoring, planning and decision-making processes. However, the burden imposed on the human user of having to interpret large amounts of data at the lowest levels of context has resulted in a wasteful and often ineffective application of valuable and scarce human resources. In particular, it often leads to late or non-recognition of patterns, overlooked consequences, missed opportunities, incomplete and inaccurate

assessments, inability to respond in a timely manner, marginal decisions, and unnecessary human burn-out. These are symptoms of an incomplete information management environment. An environment that relies entirely on the capture of data and the ability of its human users to add the relationships to convert the data into information and thereby provide the context that is required for all effective planning and decision-making endeavors.

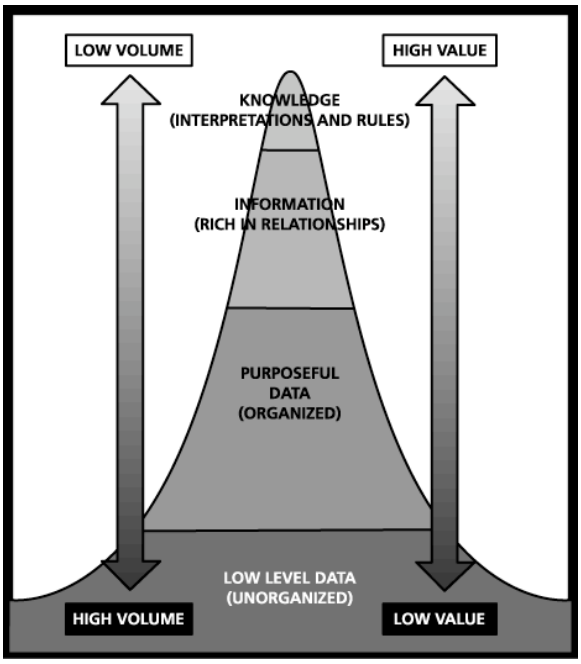


Figure 1: Transition from data to knowledge

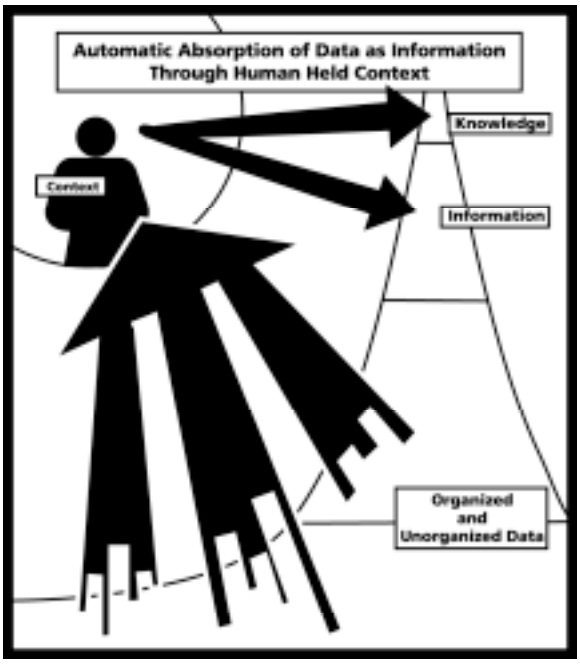


Figure 2: Human interpretation of data

A more complete information management environment considers data to be the bottom layer of a three-layer architecture, namely:

> A ***Data Layer*** that integrates heterogeneous data sources into accessible and purposefully ordered data. It typically includes a wide variety of repositories ranging from simple textual files to databases, Data Portals, Data Warehouses, and Data Marts.
>
> A ***Mediation Layer*** that defines the structure of the data sources (i.e., logical data models), data transfer formats, and data transformation rules. The two principal purposes of the Mediation Layer are to facilitate the automated discovery of data and to support the mapping of data to information. In other words, the Mediation Layer serves as a registry for all definitions, schemas, protocols, conventions, and rules that are required to recognize data within the appropriate ***context***. The Mediation Layer also serves as a translation facility for bridging between data with structural relationships (e.g., based on a logical data model) and information that is rich in contextual relationships.
>
> An ***Information Layer*** that consists of many functionally oriented planning and decision-assistance software applications. Typically, these applications are based on internal information models (i.e., object models or ontologies) that are virtual representations of particular portions of the real world context. By providing

context, the internal information model of each application is able to support the automated reasoning capabilities of rule-based software agents.

In such a three-layered information management environment the Mediation Layer continuously populates the information models of the applications in the Information Layer with the data changes that are fed to it by the Data Layer. This in turn automatically triggers the reasoning capabilities of the software agents. The collaboration of these agents with each other and the human users contributes a powerful, near real-time, adaptive decision-support environment. The agents can be looked upon as intelligent, dynamic tools that continuously monitor changes in the real world. They utilize their reasoning and computational capabilities to generate and evaluate courses of action in response to both real world events and user interactions.

As a result the human user is relieved of many of the lower level filtering, analysis, and reasoning tasks that are a necessary part of any useful planning and problem solving process. However, just as importantly, the software agents continuously and tirelessly monitor the real world execution environment for changes and events that may impact current or projected plans.

With this preamble, I would now like to introduce our keynote speaker, ***Richard P. Lee***. Dick Lee is the *Assistant Deputy Under Secretary of Defense (Advanced Systems and Concepts) for Interoperability and Network Centric Warfare*. His primary responsibilities include oversight of Advanced Concepts Technology Demonstrations (what we commonly refer to as ACTDs) in Command and Control, Communications, Information Operations, and Computer Network Defense. I am delighted that Dick accepted our invitation to be a keynote speaker for this year's Conference, because he has become a strong advocate for ensuring that the new ***Infostructure*** will embody and fully exploit the current paradigm shift from *data-processing* to *intelligent information management*.

Jens Pohl, Executive Director
Collaborative Agent Design Research Center (CADRC),
California Polytechnic State University (Cal Poly), San Luis Obispo

Quantico, September 10, 2003

Fifth Annual ONR / CADRC Decision-Support Workshop

September 10-11, 2003, Quantico, Virginia

The Office of Naval Research
and
The Collaborative Agent Design Research Center
Cal Poly, San Luis Obispo

"Developing the New Infostructure"

.....Homeland Security Vulnerabilities and Solutions
.....User Needs and Expectations
.....Data Models and Ontologies
.....Intelligent Software Agents
.....The Communication Infrastructure
.....Government Plans, Initiatives, and Obstacles.

Wednesday, September 10:

Time	Activity
7:30	**Check-in and Registration Begins** Registration Desk open from 7:30 AM to 4:30 PM
8:30 - 8:45	**Opening Remarks and Welcome** **Dr. Jens Pohl**, Executive Director, Collaborative Agent Design Research Center, Cal Poly, San Luis Obispo, California
8:45 - 9:45	***Keynote Address:*** **"Taking Power to the Edge: the use of Agent Technology in Decision Support"** **Richard P. (Dick) Lee,** Assistant Deputy Under Secretary (Interoperability and Network Centric Warfare) Office of the Secretary of Defense
9:45 - 10:00	**Break**
10:00 - 10:30	***"Achieving the Joint Vision: The Role of Operational Context in Future Systems"*** **Erik Chaum,** U.S. Naval Undersea Warfare Center Division Newport, Newport, Rhode Island

Wednesday, September 10 (continued):

Time	Activity
10:30 – 11:00	***" Software Agents to Reason About Situational Awareness "*** **Dr. Mark Youngren,** the MITRE Corporation, McLean, Virginia
11:00 – 11:30	***"Ontology-Based Applications for Automating Decision Support"*** **Dr. Francisco Loaiza and Dr. Steven Wartik,** Institute for Defense Analyses, Alexandria, Virginia
11:30 – 12:00	***"A Web-Centric Collaborative Decision Tool and Ontology Based on Subjective Sampling and Assessing Decision Times Among Options"*** **Dr. Jerald L. Feinstein,** The George Washington University, Washington, DC
12:00 - 1:00	**Lunch**
1:00 – 1:45	***"Demonstration of a Typical Ontology-Based Collaborative Agents System: SEAWAY"*** **Col. Tony Wood (USMC Ret.) and Dr. Jens Pohl**, Collaborative Agent Design Research Center, Cal Poly, San Luis Obispo, California
1:45 – 2:15	***"Countering Threats to America's Public Telephone Networks"*** **Dr. Sujeet Shenoi**, University of Tulsa, Tulsa, Oklahoma
2:15 – 2:45	**"*Internet-Telephone Network Convergence: Themes and Security Issues"*** **Dr. Anthony Meehan,** University of Tulsa, Tulsa, Oklahoma
2:45 – 3:00	**Break**
3:00 – 3:30	"***Multi-Agent Modeling of the Urban Operational Environment"*** **Dr. Frederick J. Diedrich**, Aptima, Inc., Woburn, Massachusetts
3:30 – 4:00	"***Ontological Approaches for Semantic Interoperability"*** **Michael Zang,** CDM Technologies, Inc., San Luis Obispo, California
4:00 – 4:30	**"*The Development of Complex Adaptive System Based Decision Support Systems"*** **Dr. John Hummel,** Argonne National Laboratory, Argonne, Illinois
4:30	**(CLOSE DAY ONE)**
5:00 – 7:00	**Social in Ballroom 3**
7:00 – 9:00	**Speakers' Dinner in Ballroom 4 (by invitation)**

Thursday, September 11:

Time	Activity
7:30	**Check-in and Registration Continues** Registration Desk open from 7:30 AM to noon
8:30 - 8:45	**Welcome and Announcements** **Dr. Jens Pohl**, Executive Director, Collaborative Agent Design Research Center, Cal Poly, San Luis Obispo, California
8:45– 9:45	***Keynote Address: "Information in the Execution of the Homeland Security Mission"*** **Dr. Ronald Maehl**, Homeland Security and Services Division, Integrated Defense Systems, The Boeing Company, Seal Beach, California
9:45 – 10:00	**Break**
10:00 – 10:30	***"A Paradigm Shift for Information Technology "*** **Robert Kidwell,** Vice President, ManTech Advanced Systems International, Inc., Fairmont, West Virginia
10:30 – 11:00	"***Leveraging a Global and Adaptable Infrastructure"*** **Mr. Mark Adams,** Chief Technical Officer, Iridium Satellite LLC, Leesburg, Virginia
11:00 – 11:30	**"*Wireless Sensor Networks - Technology for Detection and Protection"*** **Mike Horton,** Founder and CEO, Crossbow Technology, Inc., San Jose, California
11:30 – 12:00	***" Evolving Systems to Support the Global Information Grid"*** **Dr. Thomas McVittie**, Jet Propulsion Laboratory/Caltech, Pasadena, California
12:00 – 1:00	**Lunch**
1:00 – 1:45	***"SecureOrigins: National Strength Through Security and Competitiveness"*** **Hector Holguin,** *e-plaza,* Holguin Group, El Paso, Texas
1:45 – 2:15	***"A Data Strategy for the 'Virtual Border': Repurposing Commercial Information for Homeland Security Risk Assessment".*** **Robert Quartel**, Chairman and CEO, and **Eric Chasin**, CTO, FreightDesk Technologies, Dunn Loring, Virginia
2:15 – 2:45	***" A Regional Supply Chain Simulation Model using Artificial Intelligence"*** **Dr. Larry Mallon**, Director, CITT, Long Beach State University, California
2:45 – 3:00	**Break**

Thursday, September 11 (continued):

Time	Activity
3:00 – 3:30	***"Understanding Operational Collaboration in the Fleet"*** **Dr. Sunoy Banerjee**, Center for Naval Analyses, Alexandria, Virginia
3:30 – 4:00	"***Understanding and Applying the Cognitive Foundation of Effective Collaboration"*** **Dr. David Noble,** Evidence Based Research, Inc., Vienna, Virginia
4:00	**Workshop Wrapup** **Dr. Phillip Abraham,** Office of Naval Research, and **Dr. Jens Pohl**, Executive Director, Collaborative Agent Design Research Center, Cal Poly, San Luis Obispo, California
	(CLOSE DAY TWO)

Dr. Phillip Abraham
Logistics Program Office
Office of Naval Research

Dr. Abraham is a Scientific Officer at the Office of Naval Research (ONR). For the past eight years, starting in 1994, he has managed the ONR Science and Technology (S&T) Logistics Program. A major endeavor during these years was the introduction of S&T projects in a program that at the time depended on old technologies. In this he was guided by the view that the goal of military logistics is readiness everywhere , at all times. Toward this goal he introduced state-of-the-art sensors (e.g., MEMS), intelligent agents for decision support systems, and other innovations in both hardware and processes. Under his management the Logistics Program has addressed a host of areas that needed S&T attention. These included Maintenance (where sensor monitoring and diagnostics of systems replaces fixed schedule checkups and overhauls), Underway Replenishment (the goal being operation in sea states 3 and higher via technical improvements to existing crane systems, as well as the development of new systems that will eventually replace the conventional cranes), Amphibious Logistics (Seabasing is the major goal here and the tools that will enable the integration of the sea and shore operations are the SEAWAY and LOGGY projects that have received support from both the Navy and the Marine Corps), Naval Facilities (the major thrusts in this area were the operation of the naval bases, the rehabilitation of the deteriorating naval piers, the design of modular hybrid piers, and the design and construction of high performance ordnance magazines), Decision Support Systems (the goal in this area is to provide to the CO, at any level of command, a decision system based on state-of-the-art collaborative intelligent agents and tailored to the needs of that level), and Integration (the goal here is the integration of all the systems on a single navy platform, a squadron, a battle group, a fleet, &c., that will result in the highest achievable state of readiness. A current project, "Mission Readiness Analysis", addresses the challenge of systems integration on a single platform).

Dr. Abraham joined the Office of Naval Research in 1989 as a member of the Mechanics Division where he was in charge of the ONR 6.1 Structural Acoustics Program, the goal of which was minimizing the emission and scattering of sound by submarines. Based on his own prior work while employed by Raytheon Co. (see below), he introduced the idea of working in the time domain in computations related to the response of complex elastic structures to internal and external excitations. This allowed the computation of the response of models of submarines with internal structure in (almost) real time and reduced the demands on computer hardware. This work was performed at the University of Texas (Austin) and Stanford University (Palo Alto) using the most sophisticated computational techniques (of the time) for large scale problems.

From 1982 until 1989 Dr. Abraham was a member of the Naval Research Laboratory where he did research on fluid-structure interactions, and on wave propagation phenomena. He studied the propagation of acoustic waves in inhomogeneous and random media, and showed how to obtain results, to all orders, for both weak and strong inhomogeneities. This work, and work on reflection tomography, were motivated by the need to detect passively or actively targets in regions of the ocean that are contaminated by random distributions of biological and other scatterers.

In 1974 Dr. Abraham started working at the Naval Underwater Sound Laboratory in New

London, Connecticut. There his research dealt with underwater acoustics, focusing on detection and localization of underwater targets. Among other topics, he determined the influence of size on magnetic anomaly detection (MAD) of ferromagnetic targets (such as submarines). In addition he, and Dr. H. Moses, used inverse scattering theory to generate new families of sound velocity profiles (in the ocean) for which the wave equation has exact solutions. These were useful later on in determining acoustic wave propagation in the arctic ice cap. This work also led to concurrent results for potentials appearing in the Schrodinger equation of Quantum Mechanics. One of these potentials, a nontrivial modification of the harmonic oscillator potential, has been referred in the literature as the Abraham-Moses potential.

From 1970 until 1974, Dr. Abraham was an Assistant Professor of Physics at the University of Connecticut, where he taught and worked on Nonlinear Dynamics problems related to solitons.

During 1968-1970, Dr. Abraham was employed by Raytheon Company in New London, Connecticut. There he worked on acoustic imaging in fluid media using an exact analytic approach for solving wave equations in the time domain. A concurrent laboratory experiment yielded a visual image, on a TV screen, of an insonified, submerged object. At that time, it was the first such image generated with acoustic waves.

In 1966 Dr. Abraham was granted a Postdoctoral Research Associateship by the National Research Council. Located at NASA's Goddard Space Flight Center, he worked on propagation of charged particles (originating from solar flares) through the interplanetary magnetic field. The results of the theoretical work matched quite well with experimental results obtained from high-altitude balloon flights.

Dr. Abraham was awarded the Ph.D. in Physics by the University of Maryland in 1966. His thesis topic was in Solid State Physics, and it dealt with generating exactly solvable models of crystal lattices, which were used subsequently to check perturbation methods employed in the treatment of actual crystals. Among the results obtained was a new method of evaluating finite and infinite sums that appear in various areas of physics.

In 1960, Dr. Abraham was awarded the M.Sc. degree in Physics by the Hebrew University in Jerusalem, Israel. His Master Thesis (in atomic spectroscopy) dealt with the computation of the energy levels of isoelectronic sequences of atoms in various configurations. The results of these computations reside in the tables published during the sixties by NIST (then NBS), under the editorship of Dr. Charlotte Moore.

Mark D. Adams
Chief Technology Officer
Iridium Satellite, Leesburg, Virginia

Mark D. Adams is chief technology officer of Iridium Satellite LLC, providing global satellite voice, paging and data solutions. In this position, Mr. Adams is responsible for system enhancements, product development and new service strategy related to voice, paging and data offerings. He has over 15 years experience developing enhanced capabilities and services for wireless systems including satellite, cellular/PCS and 802.11 networks.

Prior to joining Iridium Satellite LLC, Mr. Adams served as the manager of the Networking and Communications Engineering Center at the MITRE Corporation focused on the research, development and

implementation of communications and networking systems for the department of defense. Mr. Adams and his team lead a series of vulnerability assessments on mobile satellite system architectures. His team subsequently led the development of the government mobile satellite services gateway and developed numerous enhanced satellite capabilities for the DOD. In addition, Mr. Adams and his team focused on emerging technologies within digital personal communications services, local area networking infra-structures, as well as a variety of traditional military communications systems and networks.

Since joining Iridium Satellite, Mr. Adams has developed and introduced two highly successful data services over Iridium, making internet access ubiquitous and global, and providing a revolutionary global messaging system.

Mr. Adams holds a bachelor's degree in physics from the University of Virginia and a master's degree in electrical engineering from Virginia Polytechnic and State University.

Dr. Sunoy Banerjee
Center for Naval Analyses
Alexandria, Virginia

Dr. Banerjee has been working on issues regarding the role of information technology (IT) in the Navy. Recent projects have examined the use of IT for battle group command and control, metrics that gauge the performance of Navy networks/ applications, and providing guidance to the fleet about how to effectively leverage its investment in IT to improve operational effectiveness. These efforts have provided Dr. Banerjee with the unique opportunity to collect operational data and observe how these systems are used in an at-sea environment.

Eric Chasin
Chief Technology Officer, FreightDesk Technologies, Dunn Loring, Virginia

As the Chief Technology Officer for FreightDesk Technologies, Mr. Chasin personally oversees the development of their software solutions as well as the technical solutions implemented for each of their clients. He is currently involved in delivering solutions to a large US Federal Government client related to their build of an architecture and data model to supportlogistics tracking globally. Mr. Chasin has been involved in systems integration consulting and management for seventeen years with a focus onlogistics and transportation for ten years. Mr. Chasin received a degree in Engineering from the University of Maryland in 1985.

Erik Chaum
U.S. Naval Undersea Warfare Center
Newport, Rhode Island

Erik Chaum is a member of the Combat Systems Department at NUWC Division Newport, where he works on a wide range of advanced concepts. He serves as a Naval Sea Systems Command (NAVSEA) representative in the Systems Command Liaison Office at the Office of Naval Research (ONR) and is the U.S. National Leader of The Technical Cooperation Program (TTCP), Maritime Systems Group, Technical Panel One. He has lead NUWC's recent virtual submarine participation in Fleet Battle Experiments Golf, India, Juliet and Kilo. He is a graduate of the U.S. Naval Academy (1977) and the Management of Technology program at the Massachusetts Institute of Technology (1984).

Dr. Frederick J. Diedrich
Cognitive Systems Group
Aptima, Inc., Woburn, Massachusetts.

Frederick Diedrich is a Cognitive Psychologist and Leader of the Cognitive Systems Group at Aptima, Inc., in Boston, MA. He has expertise in the areas of human performance, perceptual-motor processes, and decision-making. Much of Dr. Diedrich's work focuses on the use of dynamic systems theories to understand complex behaviors. At Aptima, Dr. Diedrich is managing a range of research projects related to modeling, experimentation, and training. He is managing a project to develop a complex systems modeling tool for the analysis of urban operational settings. In addition, he is managing a project that is focused on using intelligent agents as teammates and as tutors to enhance the training of teamwork and communication skills. Prior to joining Aptima, Dr. Diedrich was a Scientist at Exponent – Failure Analysis Associates. He studied issues concerning the prevention and causes of accidents associated with a wide range of consumer products. While a Post-doctoral Research Associate at Indiana University, he investigated the influence of perception and action on decision-making, using the relatively unskilled infant action system as an avenue to understand basic decision-making processes. Dr. Diedrich holds a Ph.D. in Cognitive Science and a M.Sc. in Experimental Psychology, both from Brown University. In addition, he holds a B.A. in Psychology from Hamilton College.

Dr. Jerald L. Feinstein
The George Washington University
Washington DC

Dr. Feinstein is a professor at the George Washington University and former Visiting Fellow at Harvard. He serves on corporate advisory boards, teaches graduate courses and conducts research in next generation information technologies, artificial intelligence, neural nets, and web centric collaborative decision ontology.

Consultant to Fortune 100 Companies and Government Organizations and was formerly associated with Booz, Allen & Hamilton, The Stanford Research Institute of Stanford University, The Naisbitt Group, and MITRE.

Recognized author - - editorial board of several peer reviewed technical journals, delivers a series of technology seminars presented throughout the world, invited lecturer at AOL, Harvard, Princeton, University of Pennsylvania, Oxford University, University of Virginia, and American University, and US Editor of The Expert Systems Journal. Invited speaker for the National Science Foundation's Senior Leadership Retreat on web centric, agent-based methods for early recognition of technology trends, AOL's Innovation speaker series on web centric methods for collecting and processing member preference metrics, Homeland defense conference on web centric intelligence collection, and related presentations.

Hector Holguin
Founder and CEO, e.holguingroup
El Paso, Texas

Hector Holguin is founder and CEO of e.holguingroup LLC of El Paso, Texas. This firm develops a pioneering 3-D virtual model for the Internet. In 2002, the e.Plaza platform evolved to serve the goals of Border Security and Border Prosperity, which will be applied to major crossings on the U.S.-Mexico border.

Prior to founding e.holguingroup, Mr. Holguin was President and CEO of Accugraph and recently retired as Chairman

of Board. Accugraph was recognized worldwide as a leading software provider for the Telecommunications and Network Management Industries.

During the 1970s and 1980s, Mr. Holguin founded Holguin Corporation, pioneer in Computer-Aided Design (CAD) applications. In 1972, Holguin introduced the first CAD desktop workstation. In the 1980s, HolguinCAD became the leading technical software for Hewlett Packard computers. HolguinCAD/HP established a global base of over 10,000 installations of its products and automation services.

In the 1960s, as Aerospace Project Engineer at Douglas Space Systems Center, Huntington Beach, California (now McDonnell-Douglas Space Center) Holguin was responsible for one of the largest test programs to be conducted at the Space Center. This extensive two-year testing program certified the Saturn Space Vehicle's Thrust Structure for flight (first Apollo missions).

Mr. Holguin holds a Bachelor of Science in Civil Engineering degree from The University of Texas at El Paso, and a Master of Science in Engineering degree from The University of Texas at Austin.

Mr. Holguin's honors and awards include: Engineer of Year, El Paso-Texas Society of Prof. Engineers (1979); The Conquistador Award and Key to the City of El Paso (1981);
Outstanding Citizen Award, LULAC (1981); Outstanding Ex-Student, The University of Texas at El Paso (1982); National Innovation Award from U.S. Small Business Administration, presented by President Ronald Reagan (1985); Outstanding 10-year Service Award from Hewlett-Packard for contributions to Computer and Software industries (1988); Outstanding West Texan, Texas Chamber of Commerce (1992); Nominated for position of U.S. Secretary of Energy by LULAC (1999); Legend of Texas Award (2001); and, Texas Science Hall of Fame (2002).

Mike Horton

Founder and CEO, Crossbow Technology, Inc., San Jose, California

Mike Horton holds BSEE and MSEE degrees from University of California, Berkeley, where he did pioneering work in using MEMS sensors for head tracking and motion tracking applications and holds several patents based on this work. He founded Crossbow Technology, Inc. in 1995 and has been President and CEO since that time. Crossbow has grown rapidly and steadily since inception, and is now a recognized leader in innovative MEMS-based sensor systems. The company pioneered the MEMS-based inertial system for instrumentation and guidance of UAVs, ROVs, land vehicles, and now manned aircraft, with the only FAA-certified MEMS AHRS (attitude and heading reference system). In addition Mike has brought Crossbow to a leadership position in Wireless Sensor Network Technology. Within the last two years Crossbow has fielded more than 10,000 Wireless sensor nodes to a variety of University, Government, and Industrial research customers. It has participated in the DARPA SensIT and NEST programs, providing all of the wireless sensor hardware for the NEST program. Crossbow, an ISO 9001/2000 company, has an earned reputation for innovation and for high quality products designed to exacting industrial and military standards.

Dr. John Hummel

Director, Advanced Simulation Technologies Center, Argonne National Laboratory, Argonne, Illinois

Dr. Hummel is the Director of the Advanced Simulation Technologies Center in the Decision and Information Sciences Division of the Argonne National Laboratory. He has conducted research and development efforts in the fields of climatology, radiative transfer, logistics, and intelligent decision support systems.

Robert S. Kidwell

VP/Sr. Technical Director Enterprise Integration Center (e-IC) ManTech Advanced Systems International, Inc., Fairmont, West Virginia

Mr. Kidwell serves as the Vice President/Senior Technical Director of ManTech's Enterprise Integration Center (e-IC). The center focuses on a wide range of advanced information technology and enterprise integration projects for both the Department of Defense (DoD) and international clients. These projects utilize Internet technologies to encourage remote group(s) collaboration (www.dcnicn.com); electronic commercial catalogue(s) (e-Commerce/e-Business); XML/EDI information exchange standards; Web centric foreign customs acceptance process with eleven (11) countries for the USTRANSCOM; knowledge based decision support systems; and logistics architecture modeling using dynamic analysis and supply chain management structures. For a view of these projects, see www.dcnicn.com. Mr. Kidwell also serves as Technical Chair of the NATO Integrated Technical Data (ITD) task force on IETM interoperability.

In addition to his duties as Vice President, Mr. Kidwell has served on several national/international e-Commerce and enterprise integration forums. Until December 2000, he served as the Vice Chair the Americas on the International Industrial Commission on e-Business. This multinational group addresses a wide range of issues pertaining to global electronic commerce and information technology. He is currently a senior member of the Association for Enterprise Integration (AFEI) and is the chair of their International Division.

Mr. Kidwell's career spans some 30 years as a senior program manager with vice president level responsibilities with emphasis on enterprise-wide system integration, technical and cost issues, live test demonstrations, business process engineering, computer hardware evaluations, software engineering, and computer system performance and modeling. He attended American University, the University of Hawaii, and is a graduate of the senior executive program, Fuqua School of Business at Duke University.

Mr. Kidwell resides with his wife, Helena, in Fairmont, West Virginia.

Richard P. Lee

Assistant Deputy Under Secretary of Defense (Advanced Systems and Concepts) for Interoperability and Network Centric Warfare

Richard P. Lee is the Assistant Deputy Under Secretary of Defense (Advanced Systems and Concepts) for Interoperability and Network Centric Warfare. His primary responsibilities include oversight for Advanced Concepts Technology Demonstrations in Command and Control, Communications, Information Operations and Computer Network Defense.

Mr. Lee is a native of Syracuse, New York. He graduated from the United States Naval Academy with a Bachelor of Science Degree in Marine Engineering in 1972, and from the Naval Postgraduate School, Monterey, California, in 1983, with a Master of Science Degree in Communications Engineering. He served in the United States Navy until 1999.

While in the US Navy, Captain Lee was a Surface Warfare Officer who served principally in the combatant forces, including a tour as Gunnery Officer in *USS RICHARD B ANDERSON (DD 786)* during combat operations in support of the Republic of Vietnam. His afloat assignments included tours of duty as Weapons Officer in *USS DUPONT (DD 941)*, Operations Officer in *USS EL PASO (LKA 117),* Assistant Surface Operations Officer with Commander, Cruiser-Destroyer Group Three and Commander, Carrier Battle Group Bravo (*USS KITTY HAWK (CV 63)*), and Executive Officer in *USS RAMSEY (FFG 2)*. He commanded *USS OLIVER HAZARD PERRY (FFG 7)* from 1990 to 1992.

Ashore Captain Lee served as a Military Observer with the United Nations Truce Supervision Organization in 1976, conducting peacekeeping operations in Israel and the adjoining countries. He supervised worldwide fleet communications support as Head, Current Operations Division, Naval Telecommunications Command, from 1987 to 1989. Captain Lee served as Deputy Program Director, Communications Systems Programs, Space and Naval Warfare Systems Command, and as Program Manager in the Milstar Joint Terminal Program Office. His final Navy assignment was with the Defense Information Systems Agency (DISA) as the Transition Manager for the Bosnia Command and Control Augmentation (BC2A) effort, and as the first Program Manager for DISA's Information Dissemination Management effort.

Captain Lee's personal military decorations include the Defense Superior Service Medal, the Navy Meritorious Service Medal with Gold Star, the Joint Service Commendation Medal, the Navy Commendation Medal with two Gold Stars, the Navy Achievement Medal, and various Service and campaign awards.

Following his retirement from active duty, Mr. Lee was a Director in the Information Assurance division of Galaxy Scientific Corporation, and Manager for the US Patent & Trademark Office Information Technology Product Assurance contract. He joined the staff of the Deputy Undersecretary of Defense (Advanced Systems and Concepts) in May, 2001.

Mr. Lee is married to the former Susan Merritt of Sonoma, California. They have three children and make their home in Burke, Virginia.

Dr. Francisco Loaiza

Senior Research Analyst, Institute for Defense Analyses, Alexandria, Virginia

Francisco Loaiza is a senior research analyst with IDA where he has worked for the past 16 years. Dr. Loaiza is the project leader for the Army Integrated Core Data Model (AICDM), and has been a contributor to the development of the Generic Hub data model- recently renamed the Land C2 Information Exchange Data Model (LC2IEDM)-and the Core Architecture Data Model (CADM). Dr. Loaiza received his Ph.D. in Physical Chemistry at Princeton University in 1988, and his M.A. in Chemistry from the same institution in 1984. In 1996 Dr. Loaiza received a law degree from George Mason University. Dr. Loaiza has 29 papers in the areas of data modeling, and Command and Control. Dr. Loaiza received his undergraduate education in Chemistry at Hamburg University, Germany.

Dr. Larry Mallon

Attorney at Law
Director CITT, Long Beach State University, California

Dr. Larry Mallon has compiled an enviable record of achievement and national recognition as naval officer, admiralty and maritime attorney, transportation and logistics consultant, educator, administrator, and interdisciplinary academic researcher spanning thirty-five years. A 1967 graduate of Georgetown University, he holds advanced degrees from Emory University and the University of Miami. He was the recipient of a first-ever post-doctoral fellowship at MIT-WHOI in Marine Law and Policy. He is a veteran of combat duty in Vietnam and fifteen years naval reserve service, including Legal Advisor to the Oceanographer of the Navy. Designated a Proctor in Admiralty in 1978, he is licensed to practice law in the states of California, New York, the District of Columbia and Georgia, and before the United States Supreme Court and every court of special jurisdiction.

He served as the Maritime Counsel to the United States House of Representatives for eleven years, and is the principal author of the Water Resources Development Act of 1986, the primary law of Federal navigation project development, in addition to numerous statutes codified in Titles 14 Coast Guard, 33 Navigation and 46 Shipping to the U.S. Code. He has been a Congressionally appointed Observer to the Third United Nations Conference on the Law of the Sea, and member of the U.S. delegation to the International Maritime Organization's Marine Safety and Legal Committees. He was the founding staff director to the 230 member Congressional Port Caucus in the House of Representatives.

He also served as Legal Consultant to California Select Committee on the Maritime Industry, and is the author of an entire body of law involving innovative infrastructure financing codified in the Harbors and Navigation Code. He is a nationally recognized expert in water resources infrastructure development and financing representing cities, counties and special districts throughout the State of California since 1987 in that capacity. He serves as Counsel to the California Maritime Infrastructure Authority. He is the Founding Chair of the Southern California Marine Transportation System Advisory Council to the Secretary of Transportation. He sits as a national representative on the Legal Committee of the American Association of Port Authorities.

He currently serves as founding Director of Research and Counsel to the Center for International Trade and Transportation at California State University Long Beach, a nationally designated center for goods movement research by the Secretary of Transportation. He is currently engaged in applied research for the Departments of Defense, Transportation and Homeland Research in freight movement, and in maritime, port, and global supply chain security.

Dr. Thomas McVittie

Principal Software Engineer
Jet Propulsion Laboratory, Cal Tech
Pasadena, California

Dr. Thomas McVittie is a principal software architect at NASA's Jet Propulsion Laboratory where he focuses on the research and development of communications protocols and information-centric architectures providing highly reliable distributed information services running in partially connected, long latency and low-bandwidth environments.

For the past 10 years, his work has focused on techniques for integrating data from multiple sources/systems into an information-rich representation of the real world, and on efficiently distributing the resulting information based on user-need and available network/computing resources. These techniques have been successfully applied to the Integrated Marine Multi-Agent Command and Control System (IMMACCS) and the C2 Translation Database (C2TD) developed for the USMC and ONR, and are a central part of the next-generation architecture providing information-centric services to multi-national exploration efforts on Mars.

Dr McVittie is the Chief Software Architect for JPL's Deep Space Mission Systems, principle architect of DISA's DII COE kernel, and a member of the DISA team defining Global Information Grid (GIG) Enterprise Services architecture and next generation framework for C4I systems.

Dr. McVittie holds a PhD in Electrical and Computer Engineering from the University of California at Santa Barbara. He is a member of the ACM and the IEEE.

Dr. Anthony Meehan

Center for Information Security
University of Tulsa, Tulsa, Oklahoma

Anthony Meehan is a research assistant with the Center for Information Security at the University of Tulsa. His primary interests are in the area of converged network security, in particular, VoIP networks and VoIP/SS7 interconnectivity. Mr. Meehan also maintains strong interests in computer and network forensics, and has worked with NIST and the FBI on vulnerability assessments of advanced network equipment. Mr. Meehan's honors include the prestigious Barry M. Goldwater and Department of Defense Information Assurance Scholarships. Upon completion of his graduate studies, Mr. Meehan has been selected to serve as a faculty member at the Information Resources Management College of the National Defense University in Washington, DC.

Michael E. O'Neil

Homeland Security and Services
Division, Boeing Company

Michael E. O'Neil is currently the Program Manager, Maritime Cargo Security, Homeland Security and Services Division, the Boeing Company. Mr. O'Neil comes to this position after a distinctive career of nearly 23 years in the United States Marine Corps. He served in a variety in a variety of command and staff billets providing logistics support to U.S. Marines on 5 of the 7 continents. His last tour in the Marine Corps was as the Assistant Chief of Staff, Logistics, I Marine Expeditionary Force. Of note in this position was his extensive involvement in global airport and seaport selection for the deployment and sustainment of Marine forces. Immediately following his retirement from the Marine Corps, he was designated a Research Fellow for the Logistics Management Institute (LMI), McLean, Virginia. In this capacity, he was a leading contributor to the Global Container Profiling Project (GCPP). He was also the primary author of the Operational Requirements Document (ORD) for the Army's Theater Support Vessel (TSV), and was an active participant in the analysis and reengineering of Army afloat and land pre-positioning in support of Operation Iraqi Freedom. He is a graduate of Miami University, Oxford, Ohio and the Naval Postgraduate School, Monterey, California, and a native of Minneapolis, Minnesota.

Dr. David Noble

Evidence Based Research, Inc., Vienna, Virginia

Dr. Noble is a senior scientist at Evidence Based Research. He is the Principal Investigator for EBR's ONR research into the cognitive foundations of collaboration and teamwork, and is the chief scientist for EBR war rooms. Dr. Noble has been principal investigator for numerous DOD research contracts in situation understanding, decision making, data fusion, collaboration, and command and control, drawing on techniques from mathematics, psychology, operations research, and artificial intelligence. He has degrees in Engineering Physics and Applied Mathematics from Cornell, and a post-doc in neurophysiology from University of Mississippi Medical School.

Dr. Jens G. Pohl

Executive Director, Collaborative Agent Design Research Center, and Graduate Coordinator, Architecture Department, Cal Poly, San Luis Obispo, California

Dr. Jens Pohl holds the positions of Professor of Architecture, Executive Director of the Collaborative Agent Design Research Center (CADRC), and Post-Graduate Studies Coordinator, in the College of Architecture and Environmental Design, California Polytechnic State University (Cal Poly), San Luis Obispo, California, US.

Professor Pohl received his formal education in Australia with degrees in Architecture and Architectural Science: B.Arch. (University of Melbourne, 1965) M.Bdg.Sc. and Ph.D. (University of Sydney 1967 and 1970). He taught in the School of Building at the University of New South Wales in Sydney, Australia, until the end of 1972 and then left for the US where he was appointed to the position of Professor of Architecture at Cal Poly. Following several years of research and consulting activities in the areas of building support services and information systems, Dr. Pohl's research focus today lies in the application of distributed artificial intelligence methodologies to decision-support systems in engineering design, logistical planning, and military command and control.

Under his direction the Collaborative Agent Design Research Center at Cal Poly has over the past 11 years developed and implemented a number of distributed computing applications in which multiple computer-based and human agents collaborate in the solution of complex problems. Foremost among these are the ICDM (Integrated Cooperative Decision Model) and TIRAC (Toolkit for Information Representation and Agent Collaboration) frameworks which have been applied to engineering design (industry sponsorship: ICADS - 1986 to 1991), energy conservation (US Dept. of Energy sponsorship: AEDOT - 1992 to 1993), logistical planning (US Army (MTMC) sponsorship: ICODES - 1993 to present), military mission planning (US Marine Corps (MCWL) sponsorship: FEAT, FEAT4 and IMMACCS - 1994 to present), and facilities management (US Navy (ONR) sponsorship: CIAT, SEAWAY, and LOGGY - 1996 to present).

The Integrated Marine Multi-Agent Command and Control System (IMMACCS) was successfully field-tested as the command and control system of record during the Urban Warrior Advanced Warfighting Exercise (AWE) conducted by the Marine Corps Warfighting Laboratory (MCWL) in Central California (Monterey and Oakland) during the period March 11 to 18, 1999, during a live fire Limited Objectives Exercise (LOE) held at Twentynine Palms, California, in March 2000, and during the recent Kernal Blitz Exercise held on the

West Coast in June 2001. The Integrated Computerized Deployment System (ICODES) was designated by the US Department of Defense as the 'migration system' for ship loading in July 1995. ICODES V.3 was released to the US Army in 1997 and ICODES V.5 is being released to the US Marine Corps and US Navy this year (2002).

Dr. Pohl is the author of two patents (US), several books, and more than 80 research papers. He is a Fellow of the International Institute for Advanced Studies in Systems Research and Cybernetics, and was awarded on honorary doctorate by the Institute in August, 1998, during the InterSymp-98 conference held in Baden-Baden, Germany. Professor Pohl is a Fellow of the Royal Australian Institute of Architects, a Fellow of the Australian Institute of Building, a Member of the American Institute of Constructors, and a member of IEEE.

Donald R. Quartel, Jr.

Chairman and CEO, FreightDesk Technologies, Dunn Loring, Virginia

Rob Quartel (53) is a former Member of the US Federal Maritime Commission, and an internationally recognized expert in US national maritime and transportation policy. He currently serves as Chairman and CEO of FreightDesk Technologies, named by Forbes Magazine in 2000 as "one of the ten best" in logistics on the web. The company is a leading provider of internet-based supply chain security and transportation management applications for international cargo management. The company provides its software solutions to shippers, 3PL's and to the United States government. Mr. Quartel's experience spans a wide range of energy, transportation, safety and environmental regulatory matters and a number of public-private ventures including mass transit, high-speed rail, highway, aviation and port development projects. He is a prolific and sometimes controversial writer and speaker, frequently cited in the media and called upon by the United States Congress for expert testimony. He was the leading proponent of international liner shipping deregulation, which passed in 1998, as well an advocate for reform of other US maritime laws. He has been a Lecturer at Yale University's Graduate School of Management, teaching a course on Transportation Strategy and Management; and served as a Member/Advisor to the Army Science Board on Strategic Sealift and "Army After Next" issues. Mr. Quartel is a Member of the Wilson Council at the Woodrow Wilson International Center, sits on the board of the Global Electronic Trade Association, and was a member of the Bush-Cheney Transition Advisory Committee to the US Department of Transportation. He has twice run for public office (US Congress in 1984 and the US Senate in 1992) in his home state of Florida.

Mr. Quartel has taken an active role in developing a public policy response to the issue of international container security and today serves as a technical advisor to both US Customs and the Department of Homeland Security. He was the first to publicly describe the concept of "pushing the borders out" via a "virtual" electronic data border that would allow government officials to profile cargoes prior to embarkation to the United States by merging commercially available data with intelligence information, a concept that has become one of the pillars of the President's Homeland Security Strategy.

Mr. Quartel is a graduate of Rice University and the Yale School of Management. He is married to Michela English, President of the Consumer Products Division of Discovery Communications. He and his wife have two

children, Eleanore (19) and Will (16), and currently reside in the District of Columbia.

Dr. Sujeet Shenoi

Center for Information Security, F.P. Walter Professor of Computer Science, University of Tulsa, Tulsa Oklahoma

An active researcher with specialties in information assurance, critical infrastructure protection and forensics, Dr. Shenoi is currently the principal investigator on projects supported by the National Science Foundation, the U.S. Departments of Commerce, Defense and Justice, and the National Security Agency. He is also spearheading the University of Tulsa's Federal Cyber Service Initiative that trains elite squadrons of computer security experts -- America's Cyber Corps -- who work within the U.S. government and military to protect and defend the country's vital electronic infrastructure. Dr. Shenoi was a member of the State of Oklahoma's Joint Homeland Security Task Force and serves on the FBI's National Steering Committee for the Regional Computer Forensics Laboratory Program. He is also the founder of the Tulsa Undergraduate Research Challenge (TURC), a nationally recognized program of scholarship and service. For his innovative strategies integrating academics, research and service, Dr. Shenoi was named the 1998-1999 U.S. Professor of the Year by the Carnegie Foundation.

Steven Wartik

Institute for Defense Analyses, Alexandria, Virginia

Steven Wartik has been a Research Staff Member at the Institute for Defense Analyses since 1997, where he has studied C4I specification, design, and implementation. He participated in the development of the C4ISR Reference Object Model, and has contributed to the system architecture of the Global Combat Support System and JOPES-2000. He received his Ph.D. in Computer Science from the University of California at Santa Barbara in 1983. He has published over 20 papers in C4I/M&S interoperability, software reuse, software configuration management, software engineering education, and information retrieval.

Col. Anthony Wood (USMC Ret.)

Vice President, CDM Technologies, Inc., San Luis Obispo, California

Colonel Anthony A. Wood (USMC Ret.) joined CDM Technologies in 1998 after 31 years in the Marine Corps. In 1995, he created the Marine Corps Warfighting Laboratory and served as its first director from 1995 to 1998. Colonel Wood also holds the position of Director of Applied Research with the Collaborative Agent Design Research Center at California Polytechnic State University.

In the course of his service, he has been responsible for a number of unique conceptual and practical contributions to joint warfare, naval expeditionary warfare, and our military posture in the Pacific. In 1968, he served his first tour in Vietnam as a platoon commander and then advisor to the Korean Marine Corps Blue Dragon Brigade. In his second tour in Vietnam in 1974-75, Captain Wood commanded a joint-contingent executing clandestine mission in Laos, Cambodia, and Vietnam. In January 1975, Maj General Homer Smith, USA, the Defense Attache in Saigon, had him transferred to the Defense Attache Office, where has was directed to secretly develop a plan for the evacuation of Saigon. Capt. Wood then executed that plan in April of 1975. Col. Wood has since served in a succession of infantry and recon-

naisance command billets and several staff assignments.

As the principal author of the US Navy and Marine Corps "Maritime Prepositioning Concept", he developed a detailed concept and then supervised the implementation of a national strategic response capability based on forward positioning three squadrons of specially configured climate controlled ships. Each of these squadrons contained prepackaged supplies and equipment sufficient to support a force of 15,000 Marines for thirty days. While serving as Chief of Staff Marine Forces Pacific, Colonel Wood was dispatched to Russia in 1993. There, over a two-week period of negotiations, he successfully concluded a major tension reduction agreement and multi-year exercise program with the Russian General Staff, the Commander Russian Pacific Fleet in Vladivostok, and the Commander Russian Far East Military District in Kharbovsk. Designed to relax tensions and reduce the risk of nuclear incidents in the Pacific Theater, the agreement has since been extended.

Colonel Wood's last billet was as founding Director and Commanding Officer of the Marine Corps Warfighting Laboratory from 1995-1998. Unique in its concept-based approach as well as its projection of a very different and non-traditional post cold war future, the laboratory spear headed Marine experiments to recast military capabilities in a mold appropriate to emerging future requirements.

Col. Wood's decorations include the Distinguished Service Medal (multiple awards), the Legion of Merit, the Bronze Star with Combat V, the Meritorious Service Medal, the Joint Commendation Medal (multiple awards), and the Combat Action Ribbon (multiple awards). At the time of his retirement in June 1998, Colonel Wood was the only Colonel or Captain on active duty in any service to have been twice awarded the Distinguished Service Medal.

Dr. Mark A. Youngren

Principal Operations Research Analyst, MITRE Corporation, McLean, Virginia

Dr. Mark A. Youngren is a Principal Operations Research (OR) Analyst at the MITRE Corporation, where he serves as the Senior Technical Advisor for the Center for Operations Research and Systems Analysis at MITRE's Washington C3 Center. As MITRE technical staff, he is currently the lead designer for the C2ISR portion of the Joint Warfare System (JWARS) simulation model under development by OSD(PA&E), and is also the lead in developing procedures & tools for the Center for Army Analysis that will enable them to analyze the effectiveness of C4ISR systems in the future Army Objective Force.

Before he came to MITRE, Dr. Youngren served in the US Army, retiring as a Lieutenant Colonel. He spent most of his career as an OR analyst, to include tours at the Center for Army Analysis (CAA), the Joint Staff (J-8), the Office of the Secretary of Defense, and most recently as an Assistant Professor of Operations Research at the Naval Postgraduate School. His research contributions have won the CAA Director's Award, the MORS Barchi Prize, and the Dept. of the Army Systems Analysis Award (now called the Wilbur B. Payne Memorial Award) for individual analysis. His research interests are in the area of stochastic modeling and C2ISR systems, particularly the development, analysis, and simulation of the transformation of intelligence information into situational awareness. He has a BS in Chemical Engineering, an MS in Business Administration, an MS in Operations Research, and a D.Sc. (Doctor of Science) in

Operations Research from the George Washington University. He is also an Adjunct Professor at the George Mason University, teaching graduate classes in areas such as *Decision and Risk Analysis* and *Principles of C3I.*

Michael Zang

Software Engineer
CDM Technologies, Inc., San Luis Obispo, California

Mike Zang is a Senior Software Engineer at the Cal Poly Collaborative Agent Design Research Center. He currently provides technical leadership for the Mission Readiness Analysis Toolkit of the ONR sponsored Shipboard Integration of Logistics program consults on a number of other concurrent projects at the center. Mike began his career at the research center as a core developer on the ICODES project then went on to be the technical leader and principle system architect for the ONR sponsored maritime logistics projects: CIAT, COACH, and OTIS. He introduced the use of case base reasoning at the center and is currently working in collaboration with the NRL's Intelligent Decision Aids Group, a part of the Navy Center for Applied Research in Artificial Intelligence, to extend this technology for the mutual benefit of both organizations. Mike's primary interests are in applied artificial intelligence and ontology development.

Taking Power to the Edge: the Use of Agent Technology in Decision Support

Richard P. Lee
Assistant Deputy Under Secretary
(Interoperability and Network Centric Warfare)
Office of the Secretary of Defense

I am very happy to be here and have the opportunity to address this year's ONR Workshop on Collaborative Decision-Support Systems. My remarks today will be loosely based on the essential elements of the five paragraph order for the warfighter. I am going to give you the situation that I believe I have some background on: where we are; the mission; some discussion on the challenges facing the warfighter over the next 10 to 15 years; and, finally the execution. I will conclude my remarks with some opportunities that may help meet the challenges, including a way to begin addressing those challenges by taking advantage of some recent and some on-going work. In his opening remarks Dr. Pohl alluded to the fact that the Department of Defense (DoD) has a vision for a Global Information Grid (GIG).

John Stenbit, as you know, is the Assistant Secretary of Defense for Networks and Information Integration. For those of you who may not have kept up with recent changes in DoD, I need to explain that over the summer there have been some organizational changes in the Office of the Secretary of Defense (OSD). However, John Stenbit retained his role as the DoD Chief Information Officer and is now the Assistant Secretary of Defense for Networks and Information Integration. He recently addressed the Joint Battle Management Command and Control Summit, which was a meeting between government and industry leaders, and articulated to industry DoD's vision for achieving interoperability by 2008. For those of you who may not be familiar with emerging efforts over the summer, I need to mention that there was a management decision that assigned to the Joint Forces Command (JFCOM) the responsibility of pulling together and providing joint level oversight representation of the warfighter to the joint acquisition community. JFCOM has been tasked to provide feedback to Deputy Secretary of Defense Wolfowitz by November 1 on the map that will get us to interoperability by 2008 (i.e., those elements that are needed for joint battle management command and control to achieve interoperability by 2008).

Why 2008? From my worm's eye view of the world in 2001 shortly after September 11, the anniversary of which we will observe tomorrow, Secretary of Defense Rumsfeld asked: When will the command, control and communication (C3) systems be interoperable? Somebody gave him a knee jerk response and answered, 2008! Because that is clearly the end of what is likely to be this administration and Secretary Rumsfeld's opportunity to steer the ship. Now we are in 2003, with 2008 coming at us real fast, and the question is: How are we going to make these systems interoperable? It is in this context that the summit meeting occurred and Assistant Secretary Stenbit was giving his vision of the GIG, so that industry could have a framework in which to discuss joint battle management command and control.

In his remarks, Mr. Stenbit discussed the Global Information Grid, which is essentially the web-like interconnection of sensors and applications and humans. To better describe his vision he

provided some historical perspective that I believe forms the core of the warfighter's challenge. Mr. Stenbit described the environment 25 or 30 years ago in the era of the Pueblo incident. For those of you in the room not old enough to remember that code word crisis, USS Pueblo was a lightly armed intelligence collecting ship that was captured in international waters by the North Koreans. He compared the communications and command and control capability to a telephone architecture.

Here was the scenario. When the commanding officer of Pueblo knew that he had information that others needed, specifically that he was under attack and needed assistance, he did not know who to tell. The obvious answer was for him to call his boss. His boss and immediate superior was sort of between the intelligence community and the operational community, and did not have the authority to send help. His superior in turn passed the information up the chain of command, which beautifully relayed the information on until the necessary decision maker with the authority to exercise command and control was finally informed. They came up with a plan to rescue the Pueblo. Unfortunately, that process took 36 hours, and the ship was already in port in North Korea at about the 30th hour. In other words, too little too late. So, what really happened? The telephone architecture of the C3 systems required: first, that someone with information would know that someone else needs that information; second, that person needed to know the receiver's telephone number (i.e., the communications channel to use, the call signs, the crypto keys, etc.). and finally, the receiver had to be at his telephone in order to receive the information when it came in. When that information needed to be shared with others beyond the original sender and receiver, the information exchange usually occurred up and down in a fairly structured hierarchy with the exercise of each link requiring the same knowledge of the need for information, the phone numbers and the schedule for sender and receiver availability.

Today, Mr. Stenbit says, we have evolved from that telephone architecture to a broadcast architecture. Whether that broadcast is over fiber or wires is irrelevant, it is a broadcast architecture and that information now can be placed on the broadcast and delivered to many users rapidly and simultaneously. So what is the significant difference? Well, first the information provider does not need to know the phone number of the receiver anymore. That is positive. Also, the receivers of the information do not need to be at their telephones. They can be almost anywhere to plug into the broadcast. It does require, however, schedules to be involved in that information process. The information producers have a business cycle that generates information on a set schedule, and the information receivers need to be cognizant of that schedule and the times for delivery. So to put that in concrete terms, Mr. Stenbit pointed out that a commander in Afghanistan with the mission to go into the next valley, could be reasonably confident that the needed images or geospatial products are or can be made available. But the business process that generates those products may not function in a timeline that will make them available on the broadcast to support mission planning or execution. Or, alternatively, if the business process works, the broadcast priorities may not support moving information to the forces in Afghanistan because of higher operational priorities elsewhere in the theater. There is a potential disconnect. So, while the broadcast model is a significant advance over the telephone architecture, there still are shortfalls.

Finally, Mr. Stenbit described a vision for the future architecture of network capability for information sharing. This vision revolves around what he calls the Task-Post-Process-Use

(TPPU) concept, which is a departure from the current Task-Process-Exploit-Disseminate (TPED) business process that Dr. Pohl alluded to when he was talking about how we need to be able to move information in context quickly. However, we want to do that by putting the data immediately on the network so that other entities can place the data into the context that is appropriate to their operational needs.

In this new environment the sensor data will be posted immediately on the global grid, for access by anyone who is authorized to be connected to the grid, and who needs the data. This is Stenbit's vision about "…post before process". There are four significant department initiatives under way to bring this vision into reality. First, there is the GIG bandwidth expansion (GIG BE), which will put a very high data rate communications capability into a number of nodes around the globe (i.e., an infrastructure backbone). Second, there is the Joint Tactical Radio System (JTRS), which makes available a software programmable radio so that the user can rapidly connect to the grid (i.e., connect to this backbone) regardless of the communications channel characteristics at any location where he finds himself. Today, while he does not need to know that a very high level communications channel may still need to have some crypto keys, he will need to know how to connect with whoever he wishes to talk to, and of course he cannot connect to the grid.

The third program that is being pursued at the departmental level is the Transformational Satellite Communications (TSAC) program, which will apply a revolutionary laser communications capability to satellite communications and further increase the reach of the global grid down to the remote user. Network-Centric Enterprise Services, which at a high level are being called the GIG Enterprise Services (GES) but are destined to re-emerge as Network-Centric Enterprise Services when some programmatic pieces are in place, will provide the mechanisms to connect providers and users to the grid. Recall the problem with the telephone architecture where the user needed to know the telephone number. Well, NCES eliminates the need to know the telephone numbers and it also provides services for publishing, discovering, subscribing to, and retrieving data, operating and managing the grid itself and then providing some necessary security features.

The fourth major pillar, if you will, of the Stenbit vision is the information assurance and protection capability that would both defend the grid (i.e., provide defense for the information both at rest and in transit) and protect the users from an electronic cyber perspective.

So it sounds like we are finally headed for the warfighter's information nirvana. You have this great infrastructure coming together and some people are saying: What's the challenge? Well the mission, if you will, is to implement a complete global information capability including moving on with the business of implementing the DoD Net-Centric Data Strategy that Dr. Pohl spoke of. We must ensure that the warfighter is better off in the future than he is now with the current broadcast model. In other words, he or she must have rapid understanding shared across echelons and between peers focused on those essential few pieces of information needed for sound and effective decisions. The warfighter has no time nor patience for dealing with lots of irrelevant and distracting and confusing data. I believe the real challenge to achieving the GIG vision is in respect to the political and cultural aspects of data. Now let me explain that with reference to the telephone architecture. Data exchange was slow, relative to the user's ability to

think. Those who had data, which they had developed into information, did so in context. They knew that someone else needed that information and they were mostly challenged in their ability to move that information to others who needed it. In the broadcast model, data are available quickly. Much more quickly than most of us can comprehend and understand in a particular situation. We compensate by collaborating. We put together multiple thinking machines (i.e., humans and their brains) so that we can quickly make sense of the data coming to us. The challenge then is dealing with the volume and speed of data that we can expect to be available to us, both up, down and across echelons and in both joint and coalition environments. We collaborate now to understand the situation and decide what to do. I do not believe we are yet into information overload, but we are on the verge of being overwhelmed by data. At this point it is important I think to make sure that, everyone understands the difference when I use the terms "data" and "information." I believe that data becomes information when it is placed into context and I am sure that most of you agree with that statement. If I told you that a stock closed yesterday at a certain price, I have provided you only a single piece of data without context. It would be difficult for you even to decide to gather additional data. However, if I added what the price was a month ago, what earning estimates are up, that the market assessment expects strong performance in the associated sector, you now begin to have information because I have provided some additional data that provides context. With other information you can decide to act to buy or sell or hold, or to seek more information. The additional data tends to build your understanding of the information.

Data without context can be next to useless. It may even slow down one's ability to act because one has to gather additional data to understand the situation and to then place the original data into context. I believe that this problem is the basis for our substantial investment in efforts to collaborate. We must combine our context processing powers (i.e., our brains) to deal with the increasing pace of data collection and generation, with the pace of operations in which we need to make decisions, and from an OSD level of perspective with the cost of doing business. I believe that the manpower implications of needing to collaborate amongst human beings in order to organize and make sense of data, are absolutely scary. We do not have the money to buy and train the people to understand the data that they are looking at. We need to provide some structure to that data. There are those who would tell us that the information about the impending attacks on America that occurred on September 11 (2001) were all available. If only the right people had been able to share the right pieces of information with each other they could have predicted the attack. At least that is what some people will tell us.

The challenge of implementing the global grid is to shield the warfighter from the potentially overwhelming volume and pace of data. In Stenbit's talk at the Joint Battle Management Command and Control Summit, he said the first step for achieving the capability potentials of the global grid is for the domain users to define the information needs and data schemas within their community of interest. Now what did he mean by that? It means that we must get on with implementing what he signed out in May (2003) as the DoD Net-Centric Data Strategy. It means that the participants in each community of interest must document the context for the data in their domain. They carry that context now mostly in their heads. There are very few communities who have actually sat down and documented that context. It is in that context that data are turned into information, and through this context the different communities interact to support mutual goals. Let me give you an example. If a commander or operational staff officer asks a

meteorologist for a forecast, he might learn that it is expected to rain at 4-6 mm per hour for the next 6 hours, followed by a backing wind and dropping temperatures. The forecast is accurate and perfectly in line with the question. But in response that staff officer may restate his question more precisely. What he really wanted to know was whether the forecast might suggest that his tanks need to stay on the road rather than going across the fields based on how heavy the expected precipitation might be. The meteorologist could then work within his community's context to evaluate weather-related data to generate information which he is then able to communicate to the staff officer in the context of the situation, to provide the answer to the real question. And, note, there are multiple communities of interest and different semantics or contextual settings at play in my example. Each community of interest needs to completely understand or function in the other's domain. But each needs to be precise at the interface for information exchange, because less than precise definition will lead to confusion, misunderstanding and delay in comprehending a situation and subsequent decision-making.

So now we have the challenge facing the warfighter, namely potential overwhelming data with an associated need to share information as rapidly and precisely as possible. The challenges that I see for the warfighter are in defining and documenting the relationships that provide the context so that he operates in an information-centric environment.

We have some emerging solutions, namely the Global Information Grid which provides both the challenge and the solution to part of the problem. John Stenbit challenged system developers to build toward the plan to envision the environment. He advanced a concept of assuming the environment exists, and to develop capabilities to take advantage of he planned advancements. For example, he suggested that the application developers work to build applications that can use Internet Protocol Version 6 (IPV6) capabilities. If operational testing and evaluation events occur before the completed implementation of IPV6, then adjustments in test events should be proposed. In that way, when the implementation of IPV6 is complete, the adjustments can be removed and the application or capability can function as planned. The benefit to the communities at large is more rapid achievement of the envisioned global grid.

The current normal approach for the program manager is to guess how much of the desired or expected capability will actually exist when the program reaches a test event, and then to build to the capability that he expects to see in that test environment. That hedges him for success but leaves the application short of the intended environment. Consequently, the intended environment is not realized as quickly as it could be, because people are not demanding its implementation. Similarly when Stenbit signed off on the DoD Net-Centric Data Strategy in May of this year, he was in fact providing very specific guidance under the Department's approach to enabling the rapid sharing of information across communities of interest. The challenge for the technologist here at the workshop and for the warfighters is to embrace the opportunities included in that guidance and strategy.

So you are probably thinking, what is the connection when I was talking about data and context and then shifted to this other issue about advancing the GIG and Stenbit's vision. The Joint Battle Management Command and Control effort that I spoke of earlier is aimed at achieving interoperability by 2008. It touches a number of DOD initiatives: Global Information Grid Enterprise Services (GES); Standing Joint Force Headquarters; a Deployable Joint Command

and Control or DJC2 capability; and, the Joint Command and Control (JC2) which is the migration of the Global Command and Control System. It does redefine what we need in or from those various initiatives. I believe the effort to apply context to data is still missing. When I go to some of these high level meetings I do not hear much discussion about how the DoD Net-Centric Data Strategy will be made fundamental to the program that is being discussed (e.g., JC2 or DJC2). What this means in my view is that if we are successful in achieving the connectivity, the interoperability and the ubiquity of the vision for the GIG and all of its associated capabilities, but have not moved to implement the data strategies and the resultant information-centric architecture that addresses data in context, then we will only serve to overwhelm the warfighter in a world of increasingly complex decision-making environments.

The good news, I believe, is that there has been some significant thinking in this area. This will help to advance the warfighter to take advantage of emerging capabilities. So now we are to the execution stage of the five-paragraph order. The Department has been engaged in something called the semantic web. I am sure that a number of you in this room have worked on pieces of that as well. You probably have a much better and more complete understanding of what the semantic web means than I do, and I expect to hear discussions during this Workshop about advances in this area. I know that academic institutions and the services are making progress in capturing the promise of smart agent technology that can assist decision-making in a context rich information environment. And the good news is that we are learning that we do not have to work toward a single definition of context for data. I believe it is important, however, for the communities of interest to document their community context and to pay particular attention to the nomenclature at the interfaces between communities.

There is significant progress in the command and control area. A consortium of NATO countries has collaborated to define the nomenclature for C2, starting from the US Army's engagement with the NATO Army Tactical Command and Control Information Systems or ATCIS effort. It documented an information exchange data model for the purposes of data exchange between LAND C2 systems. During the 10 years of its development, the information exchange data model has expanded from its land roots to include almost all military capabilities and tasks except for some space-related stuff. This data model has been ratified as the recognized business model for command and control within NATO (i.e., as the C2 Information Exchange Data Model (C2IEDM)) under NATO agreement 5523. The configuration management of the C2IEDM, or the Generic Hub as it is often called, has recently moved to the Multilateral Interoperability Program or MIP, which is a NATO effort.

In addition, tomorrow Lt. Col. Scott Hoffman of the Marine Corps, assigned to the Joint Staff Division for Interoperability (J6I) will brief the the Generic Hub to the XML Repository Managers Working Group for validation of those XML tags for use by the coalition enterprise level. Why is this important? Well, the smart folks who participated in building the Generic Hub, and I believe that some of them from the Institute for Defense Analysis (IDA) are in the room today and will speak here today or tomorrow, included some necessary hubs for communicating context with the data and the C2IEDM data model. And that will allow the application of smart agent technology being developed by the services and by academia. Smart agents can work on the data in context, watching for relationships between objects in the data to be made or broken. In fact, some significant work in this area has already taken place by the

Marine Corps in the Integrated Marine Multi-Agent Command and Control System (IMMACCS) and in SEAWAY, the associated sea-basing logistics capability, and I think we will hear about that this afternoon.

So why don't we get the developers and the users to start jumping up and down and demanding context for data? I think it is because the users have not yet seen the potential for the future. I think we, who are dedicated to finding technology and applying it to warfighting problems, also have discovered that understanding the concepts such as the application of ontologies and intelligent agents is a challenging intellectual process. We find that the development and use of ontologies and agent-based tools requires focused concentration. The Warrant Officer and NCO who must ensure that his people are trained, fed, and paid, finds it difficult to imagine sometimes how IMACCS or SEAWAY, or any other program will specifically help them.

The Pentagon office that I work in oversees Advanced Concepts Technology Demonstrations (ACTD). We have already undertaken some ACTDs like Extending the Littoral Battlefield (ELB) and the follow on Joint Task Force Live Area Relay Network or JTF Warnet, for example, to demonstrated ontologies, intelligent software agents, and visualization support for the warfighter. Commanders were enthusiastic about the potential of the capabilities they saw, but I believe that the relationship between what they glimpsed and the capabilities and technologies that we will be discussing in this Workshop is still pretty foggy for them. You know, it is difficult to understand or recognize or even appreciate that what you are seeing on a screen in the command center is functioning because you have got software agents working in the command system.

I recently had an opportunity to see a presentation by one of the major defense integrators. He did a great job of showing how his operational planning tool would fit together with some ISR tools and some logistic support applications. However, when I asked him at the end of the demonstration if he had an ontology for the data in his application, his answer was no. This tells me that all of the tools and activities that were operating were operating at the application level. He was putting data in context so that it would present nicely on the screen at the application level. The difficulty with that approach is that we all have to buy the same applications from the same major defense integrator so that we can all see the same information and have the same understanding of the situation. Alternatively, we will see differing views of the same data and have to collaborate to understand why we are seeing differing views until we have resolved those differences and better understand the context.

The reason why this is important to me and why that little excursion was necessary is that I am developing a plan, or attempting to develop a plan with a number of folks helping me, for a fiscal year 2005 Advanced Concepts Technology Demonstration (ACTD) focused on command and control. The charge from my boss is to build an ACTD that is linked to the new C2 functional control board, which is the revamping of the JROC process. For those of you who are not aware, and we can certainly talk about this at a break if you are more interested, the JROC process has been reorganized and there will no longer be a JRB and a JRP. It will simply be a Functional Control Board (FCB) that will feed the appropriate things up to the Joint Requirement Oversight Council (JROC). The FCB's activities have also now embraced the Joint Warfighting Capability Assessments or JWCAs and, therefore, the C2 FCB should have cognizance over gaps that have

been discovered in their analysis of warfighting capabilities, and will also on the other hand be able to screen proposals going to the JROC through this functional analysis of capability shortfalls. I would like to undertake an ACTD that builds on past ACTDs that have explored ontologies and agents. An ACTD that will facilitate integrating into the GIG some of these findings along with the products, tools and capabilities that the Service laboratories and academia can provide, and demonstrate how full realization of the GIG vision can be advanced through early implementation of the DoD Net-Centric Data Strategy.

So, today and tomorrow I challenge you scientists and engineers and the technically savvy folks to explore with the warfighters in the group what their needs are. Listen carefully to the conversations and then think about how intelligent agents and ontologies and data in context can help achieve situational understanding and accelerated decision-making and help avoid the data overload problem. And if you are a warfighter, welcome to this Workshop and thanks for taking time out of your very busy schedules worrying about how you are going get all your guys to the rifle range. Do not be afraid to engage the technologists. Wrap your mind around the idea of ontologies and agents, and the potential they can bring to changing data into information and information into knowledge to help you understand and function in a complex environment.

And in closing, let me remind you that the warfighter's challenge in the next 10 to15 years will be to maintain situational understanding, shared across echelons and between peers to achieve desired strategic operational and tactical effects. Just as work expands to fill the available time, we know that the volume of data will expand to fill the available bandwidth and the GIG. The warfighter is going to need some strong computational partners to assist in focusing on essential information. Our opportunities can be found in the same efforts that are bringing the warfighter his challenges, namely the Global Information Grid (GIG). The methodologies that we need to be concerned with, I believe, are extracting information from data, using well-defined ontologies within communities of interest aided by smart agents, and demonstrating to the warfighter not only that we can do it, but that there is a good solid answer to the inevitable "so what."

Discussion:

I'm a warfighter. Here's the challenge… you mentioned an ugly word… sensor. Let me preface by saying you're remarks are spot on, thank you. I have a challenge though… if we're talking about air command and control you're right on… you've got good sensors. Sea command and control is a tad less because we have curvature of the earth problem… undersea sensors… a little more challenge there… how about the power of the people with boots on the ground? From what I understand about our command and control systems… all our sensors that pick up warm, breathing, potentially hostile bodies that could also be pregnant women having a baby… we don't have sensors that get that. We really don't have an autonomous gathering capability to pick out a picture of a ground order of a battle for a commander… and that I think is a question that I don't have an answer for. I always hear command and control and I think you're talking about air command and control, and sea command and control to the joint level, but what are we doing to address getting information for a ground guy that's not a tank, not a truck, and doesn't rotate, radiate, or emanate… thank you.

I probably can't get give you a good answer to that question. Organizationally, there are a couple of things that have occurred that probably exacerbate this problem. The decomposition of the ASDC into NII and the Intelligence community have made linking that ISR capability back into the command and control capability a little more awkward organizationally. The Joint Chiefs of Staff organization for JWICA and the new Functional Control Boards have taken that problem and stuck it into what is called situational awareness capabilities assessment, which is separate from the C2 capabilities assessment. There is significant effort continuing inside the Pentagon in support of the forward forces and blue force tracking capabilities. Even though we may not know who the white or the gray or the purple guys are, we hope we can figure out eventually where the blue guys are. Identifying where the red guys are is an awkward problem. The heart of this problem is separating the red from the white and the gray. I think there is a perception that if we can begin to get our arms around blue then at least we can identify what is gray and red. The problem for command and control is to be able to shorten the timeline for decision-making at the point of engagement. What do I mean by that? I think by putting all the data on the grid and allowing me to discover it and pull it down may work at the strategic and operational level for effects-based thought processes, such as how do I do this or how do I make this effort. However, I think at the specific point of implementation, and this is a personal opinion and certainly not a Department policy, we need to be able to provide enough information about the blue, the expected, and the potential for interaction, to help us make the decision to engage with some sort of a weapon and help us to decide how to prevent collateral damage from occurring.

You mentioned that ontologies and agent technology are going to be key for making the GIG in the future. My question for you is as follows: Besides DARPA, what future funding initiatives are coming up to actually develop this technology and then apply the technology that DARPA has already developed?

One of the purposes of the office that I'm in, and I work for the Deputy Under Secretary of Defense for Advanced Systems and Concepts, is to take the emerging technologies when they are mature enough to go to the field, and operate without a bunch of lab-coated technologists standing around to make sure the stuff works, and put them in the hands of the guys that fly the airplanes, drive the ships, the submarines, the tanks, put their feet on the ground, and give them the capability to work with. My boss has requested in the FY04 President's budget $213 million. Last year the request was $200 million, we got $208, so Congress likes the program. They understand the opportunity to take technology that is emerging and engage the warfighter, provide a capability, demonstrate that capability, get the warfighter's assessment, and then transition that into the environment. My boss Sue Paton is a peer in the DoD organizational structure of Tony Tether, who is the head of DARPA. So we take a lot of DARPA technology and insert it into warfighting capabilities. But we also reach out to the academic institutions, the services, and the service labs, to try to knit together the capabilities. The other part of what we do in ACTDs is we build this partnership. Sometimes it is a reluctant partnership. Sometimes it is a career partnership instead of a willing partnership. Sue Paton came aboard September 17, 2001. She got into the office shortly after the attack on the World Trade Center and the Pentagon, and her office is on the other side of the Pentagon so it had not been damaged. She received a mandate I believe from then Under Secretary of Defense Aldridge, who was the acquisition technology and logistics leader until recently. He stopped doing ACTDs that were science fair type projects and started doing ACTDs that could transition into programs of record. In the two

years that Sue Payton has been there she has shifted our focus. So now, if I am successful in getting an ACTD started in the FY05 time frame (seems like a long way out, but it allows the services to do their budget adjustments) and approved, then part of that planning process will be to address ontologies, software agent technology and put the ontological hooks more securely onto the C2IEDM data model. I think we are going to hear later today about the SEAWAY program. The Marines have made a great stride forward in trying to embrace an ontologically aware agent-based capability that will both accelerate decision-making and will have a positive effect on the manpower required in the future to be able to do some of these relatively routine repetitive kinds of data interactions. I believe that the planned FY05 ACTD will allow a warfighter above the lab level, above the technology level, and outside the S&T community, to see what this step does for him and say "yes, I get it." The first time I was exposed to it I didn't get it. I looked at this stuff and said: "Yeah, but how do I know this works? Show me a demonstration…" That is what the ACTDs do and we do that by providing the seed money to get this thing up into the budget, and that is part of the process of transitioning these capabilities into programs of record.

Achieving the Joint Vision: The Role of Operational Context in the New Infostructure

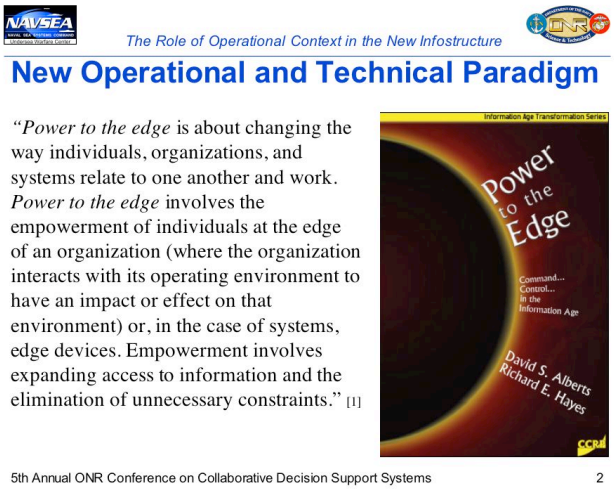
Mr. Erik Chaum
NAVSEA Liaison, ONR System Command Liaison Office
Principal Investigatgor, Naval Undersea Warfare Center , Division Newport,
TTCP, Maritime Systems Group, TP1 US National Leader

Presented at
5th Annual Office of Naval Research (ONR)
Conference on Collaborative Decision-Support Systems

Good morning. For those of you that have looked at or read "Power to the Edge," you'll know that it emphasizes agility and so you'll probably also have noticed that I've changed the title of my talk to be better aligned with today's purpose.

To give you some context to understand my perspective:

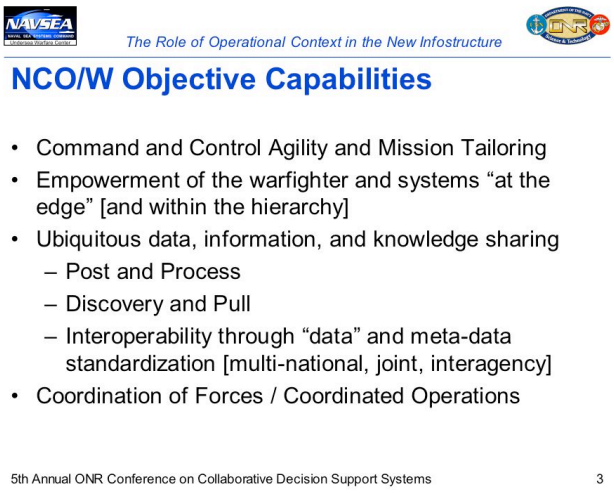
- I work part time as a Naval Sea Systems Command Liaison at the Office of Naval Research (ONR),
- I am the U.S. National Leader on the Maritime Command and Control and Information Management Technical Panel working for The Technical Cooperation Program's (TTCP) Maritime Systems Group (MAR), and
- Of late have been working with Office of the Secretary of Defense (Advanced Systems and Concepts), Joint Forces Command (J8), the Joint Staff (J6I), Navy Warfare Development Command, and Army TPIO-ABCS on interoperability issues.



For those of you who haven't seen the book *Power to the Edge*, this is the cover. There are a lot of interesting ideas inside this new book. I've chosen to emphasize this sentence; "'Power to the

Edge' is about changing the way individuals, organizations, and systems relate to one another and work." I'm going to come back to that – the notion of how organizations, and systems relate to each other. "Power to the Edge" involves the empowerment of individuals at the edge of an organization, where the organization interacts with the operating environment to impact or affect that environment. Systems can be edge devices. Empowerment involves expanding access to information and the elimination of unnecessary constraints.

So, is this really a new paradigm? This has already been alluded to by both of our initial speakers, and I want to give you my perspective on some important aspects that I think, as Mr. Lee has pointed out, have been underemphasized.



"Power to the Edge" envisions network-centric operations as improving operational and tactical capabilities, in part through: Command and control agility, mission tailoring, and empowerment of the warfighter and the systems at the "edge" of the organizational hierarchy – where the tactical action occurs. But, it is not just the "edge" we are empowering, we also want to improve the processes and capabilities that span, and exist within, the organization.

Ubiquitous data, information and knowledge sharing are central to achieving this new paradigm. We will however share information differently. Key ideas include:

- Posting and then processing - as opposed to the current paradigm were an authoritative source first processes and then posts,
- Discovery and pull – enabling the right people and systems to rapidly find relevant information, and then access it, and
- Data and meta-data standardization – enabling joint, interagency, and multinational interoperability, because we conduct operations that have this scope.

Fundamentally, network-centric operations and "Power to the Edge" address command and control - the coordination of forces, and the coordination of operations. In the most abstract sense, this is what our command and control systems enable, or are supposed to enable, us to do, to coordinate forces: Maritime, Marine, Joint, and multinational.

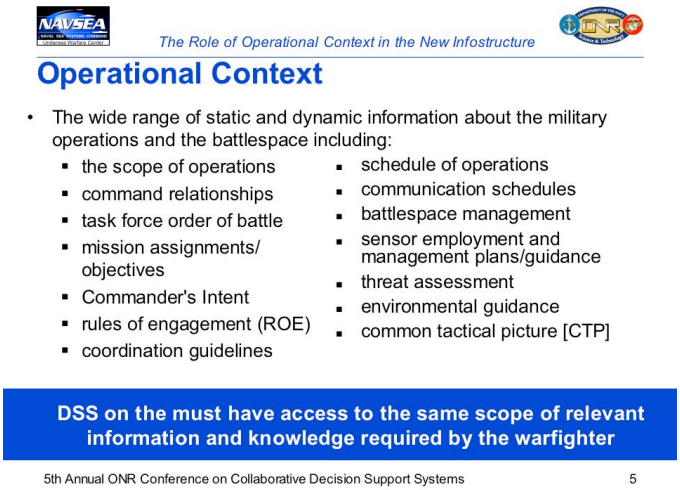
The military decision maker is the intelligent part of today's command and control or decision support system. The warfighter is as much a part of our system as any hardware or software component. (That said, at today's conference we are going to hear about some very interesting agent technologies capabilities that will lead to more intelligent software components.)

So here's a little thought experiment. Is it enough to provide a well-trained warfighter with only a perfect tactical picture? Is that enough for the warfighter to in fact make good operational and tactical decisions?

No, because warfighters need to reason about the context of an operational situation before they can make good recommendations or decisions. Importantly the same is true for classic or agent-based decision support systems.

Context or "operational context" exists today almost exclusively within the warfighter part of our command and control and decision support systems. How can the warfighter reason about that tactical scene that he is sensing if he doesn't also understand the current operational context - what is the mission, what are the rules of engagement, what are the specific assigned tasks, to whom to report, are we at war or maintaining a fragile peace, who is the enemy, who is my friend, how are responsibilities divided among our forces, what control measures are in place to guide and coordination forces, etc? The well-trained warfighter without this contextual knowledge can't reason effectively about the tactical situation or coordinate with others. He can't plan actions or select between alternative courses of action and assess which might be best.

I first performed this thought experiment when trying to understand what the US DoD Joint Vision would mean to those of us that work to deliver better command and control systems to the warfighter. How should we advance those systems? I came to the realization, through this thought experiment, that it was not enough to just collect better sensor information, but that we need to also provide/share operational context in a format that can be used by information systems – so that they are better informed.



Here in a little more detail is the kind of contextual information that I'm talking about. Our decision support systems must have access to this same scope of relevant information and knowledge – ideally the same scope that is required by people.

If an information system (software agent, application, decision support system) doesn't understand the tactical plan and associated control measures (e.g., that define where unit can be, or what area is currently a kill box) how is it going to make a complete and appropriate recommendation to the warfighter?

Today we rely on people reading operational context in messages, PowerPoint presentations, or web sites, internalizing that context, and then subsequently manually integrating context with the data presented by various sensor, command and control and combat control systems. Where is the software assistance?

To build better operational and tactical support systems we have to build better-informed systems. It's just that simple.

How do we represent this information and operational context? How do we share it? If my premise is correct then we are faced with a huge new interoperability challenge. The DoD Global Information Grid (GIG) promises to deliver a wealth of information to the warfighter, but what if our information systems can't read it? We need to identify practical interoperability methods that will enable us to achieve the rich and ubiquitous sharing of operational context.

The Domains of Warfare

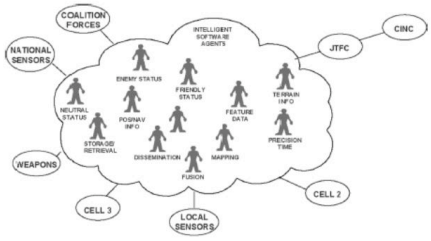
Physical Domain
where strike, protect, and maneuver take place across different environments

Information Domain
where information is created, manipulated, and shared

Cognitive Domain
where perceptions, awareness, beliefs, and values reside and where, as a result of sensemaking, decisions are made

Social Domain
set of interactions between and among force entities

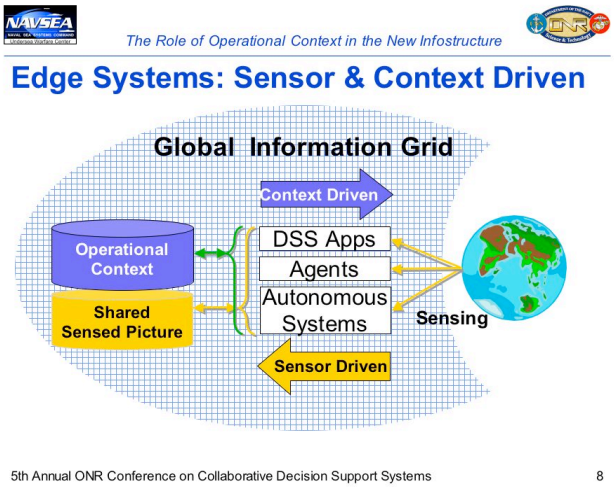
In "Power to the Edge", and actually other earlier Command and Control Research Program (CCRP) documents, the concept of "domains of warfare" is presented: the physical, information, cognitive, and social domains. Most of what I'm talking about today is addressed in the information, cognitive and domains. That said, in general when we talk about coordination of forces collaboration and the social domain are important.



- Intelligent Software Agents:
  - Relieve users of information management functions
  - Provide data fusion, information storage, retrieval and dissemination
  - Tailor information at the right time, to the combat cells needing it
  - Allow users to request information in mission specific terms
  - Provide geospatial and time information services

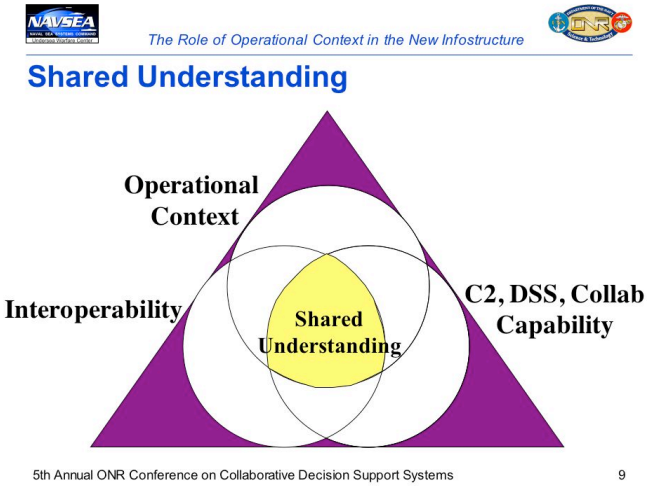
Figure 27. GIG Software Agents

This is another illustration from "Power to the Edge" that shows the GIG populated with a myriad of intelligent agents, all individually tasked to do specific kinds of things. But how do the agents know what information is relevant to their function? (Note: agents, in my frame of reference, are a type of decision support systems. I'm not saying that all decision support systems are agents or that all agents are necessarily decision support systems. They are software entities that help us by pulling information, presenting it, organizing it, prioritizing it and so on.)



The information systems that assist the warfighter at the operational and tactical levels I have characterized as applications, agents, and autonomous systems. (Note: there are a growing number of off-board air, undersea, and ground systems being built today that are becoming more and more autonomous.) Today we have a lot of systems that sense the world and with them we try to build a shared sensed picture and pass that all around. And that's absolutely necessary, and totally insufficient.

In fact today we do more than this. We build operational context (plans, orders, various tasking messages) and pass the context around often in formats that our information systems can't easily process (e.g., PowerPoint or websites designed for people to read). In the future, the operational context must be represented in a form that enables information systems to access it, understand its semantics and syntax, reason about it, produce and share it, all without people needing to getting in there and "retype it."



My thought experiment considered the Joint Vision and its objective next generation command and control systems, decision support and collaboration systems.

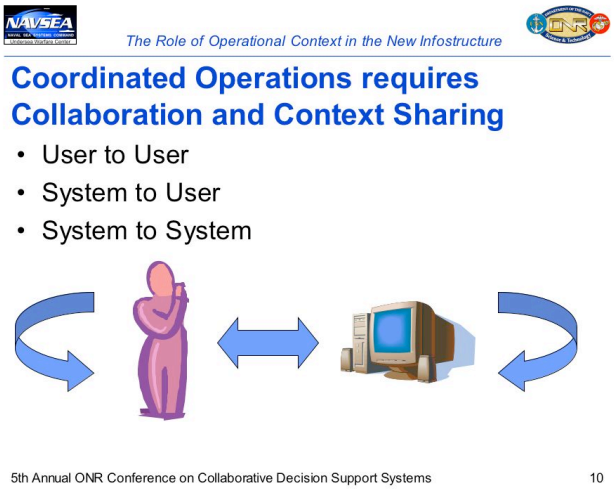
That led me to the realization that providing context to these information systems was absolutely essential when seeking to build more sophisticated, useful and automated next-generation systems.

This operational context is much richer than the traditional tracks we share today via the Global Command and Control System – Maritime (GCCS-M).

What I am speaking of is at the heart of the concepts and capabilities of the GIG – the ability to be interoperable across Services and systems. We want to write it once, i.e., put it on the GIG, and enable any appropriate GIG user to discover and use it. This is a vision that is very different from our standard approach today (point-to-point) where we have system-specific information exchange requirements and implementations – this will not scale to the GIG.

So, if you are here today representing a company, or an organization, with a system that will plug into the GIG - then you should be looking ahead to the exchange of context in a system independent form – interoperability "many-to-many", as it has been characterized by the GIG!

We're trying to get to this: "Shared Understanding" about the broader context of information and knowledge required to conduct coordinated military operations.



We have been talking about coordination of operations and that requires sharing of information, context, and in general collaboration, but that in turn requires operational, tactical and technical interoperability.

When I produce a plan and put it on the GIG I expect that "everybody" will read it, comply and provide status reports as appropriate. But when I say "everybody" I don't just mean people. The coordination of operations must occur at a number of different levels:

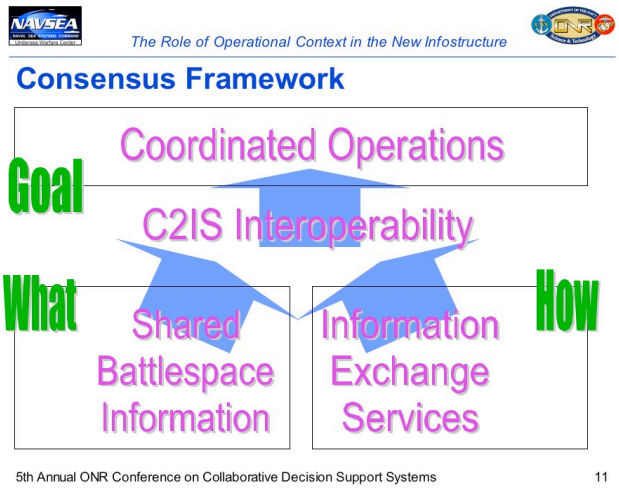
- User-to-user: Supported by classic collaboration/coordination tools – messages, telephone, email, chat, web pages,
- System-to-user: Effective and consistent methods enabling the warfighter to express intent and context into operational and tactical systems, and vice versa.

Consistent and independent of system or function to ease training and make our systems more intuitive, and

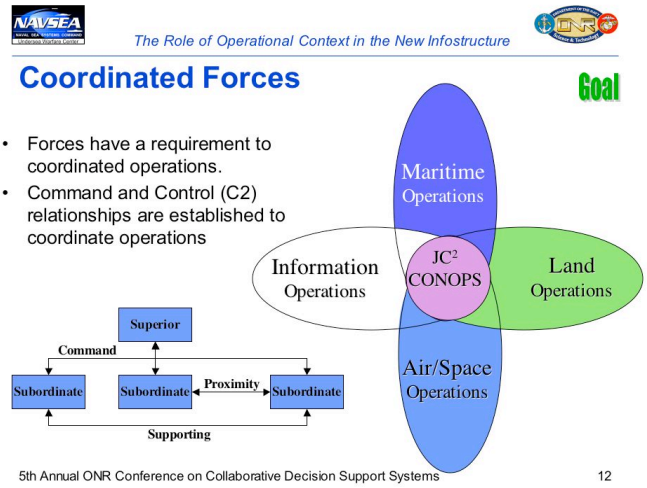
- Importantly, and where I've been focusing: System-to-system: The GIG concepts require "everybody" (people and systems) publish, and then "everybody" discovers and pulls from this common pool. This requires that we enable systems to interact with each other without building point-to-point IER's or dedicated software connections between dissimilar systems.

By the way, the good news is that system-to-system automation is precisely what the business community is working to create on the Internet. Extensible Mark-up Language (XML), a key Internet technology, enables communities of interests (COI) to build a consensus on community information exchange needs and then define the associated semantics and syntax. These COI form a namespace, a community consensus - really a simple ontology. When you agree to comply with a namespace your system will interoperate with other COI systems that uses the same namespace. This is the GIG "many-to-many" approach/solution.

An important question; is there a COI namespace for describing military operational context? We will return to this question later in my presentation.



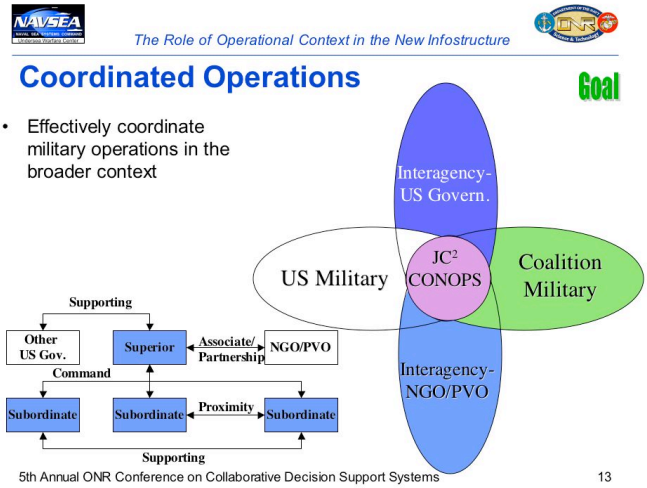
Consensus is fundamental to achieving "Power to the Edge" and effective coordination of operations. We empower people and organizations with interoperable Command and Control Information System (C2IS) tools for coordinating and collaborating. Whether by radio, chat line, or command and control systems, battlespace information and operational context must be shared. To the degree we can unambiguously communicate we have a mechanism for coordinating operations. But what information must we actually share to coordinate operations? What mechanisms will be used to make information and context flow in a timely manner to the appropriate warfighter or GIG system? To address this let's look in greater detail at each of these pieces.



Coordination of forces: This is a very general problem. Within United States military doctrine our basic concepts of command and control include a superior-subordinate hierarchy. There area also proximity, and supporting command and control relationships.

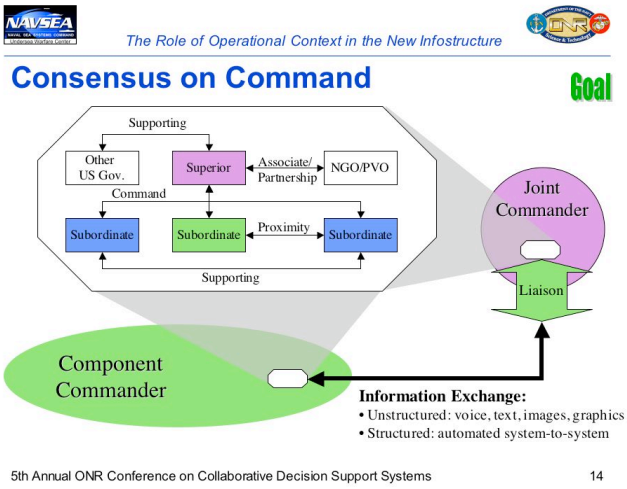
Now, this is not the only way to solve what is fundamentally a coordination problem. Let me give you a simple example. Let's play football. Okay, how many of you thought of "soccer"? Both American football and "world football" move the ball down the field. Note however, American football and "world football" use entirely different command and control processes, one is very phased and commanded and the other much more self-synchronizing. When we start talking multinational we can't assume what kind of "football" is being played!

Note that the portrayal of the Joint maritime, land, air/space, and information dimensions of the battlespace are not strictly Service oriented. Coming to a consensus about what type of "football is being played" is equivalent to establishing an operational consensus on how we will coordinate these various types of forces. This operational conceptualization and alignment are critical. At the heart of these battlespace dimensions is a core overarching need and requirement for Joint command and control consensus.



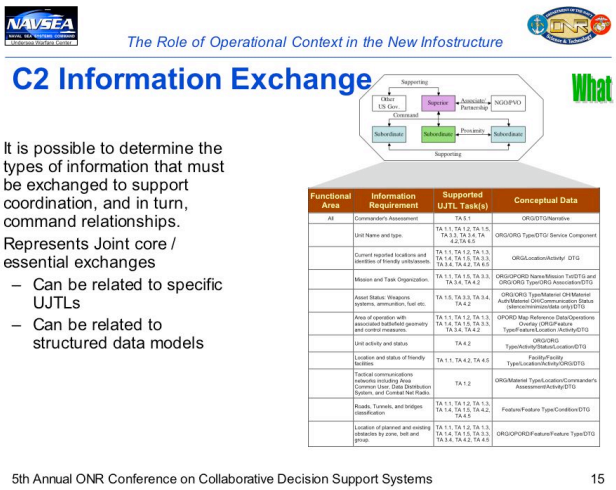
Coordinated operations span a broader context than the Joint U.S. DoD Services. Today's international situations must coordinate operations across US and coalition/allied military, and other governmental and non-government agencies. Associative and partnership relationship with non-governmental organizations are more critical than ever. Building an operational consensus across this richer set of community is very challenging! The important point to realize is that without an underlying operational command and control consensus between organizations effective coordination is difficult, dangerous, and perhaps impossible.

Said another way, operational consensus is always necessary to get things done well. Operational consensus provides the baseline for understanding and defining required command and control capabilities and supporting technical capabilities.



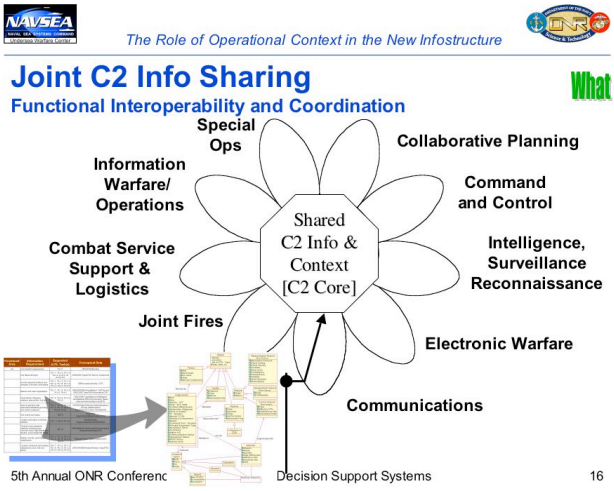
When you consider command relationships you realize is that in order to coordinate forces you must exchange information. For example, if I don't tell you the plan how can I expect you to carry it out? If I can't tell you "don't go in this area because it's dangerous", how can I expect that you will stay out? If I give you a task to do and you don't give me status, I won't know if we are accomplishing the plan. So to work together we have to exchange information.

Information can be unstructured; voice, free form text, images without metadata, some graphics. It can also be structure; USMTF, XML, databases, etc. The better and more widely understood the structure of the information being passed the better support for system-to-system information exchange and processing. Information must flow between the commander and subordinate to enable these organizations to work together. Increasingly in today's network-enabled battlespace this link is often technically accomplished using an IP WAN, LAN, or wireless connection. Often there's a liaison function, a person, who helps build and maintain the operational relationship by interpreting and explaining the information being exchanged.



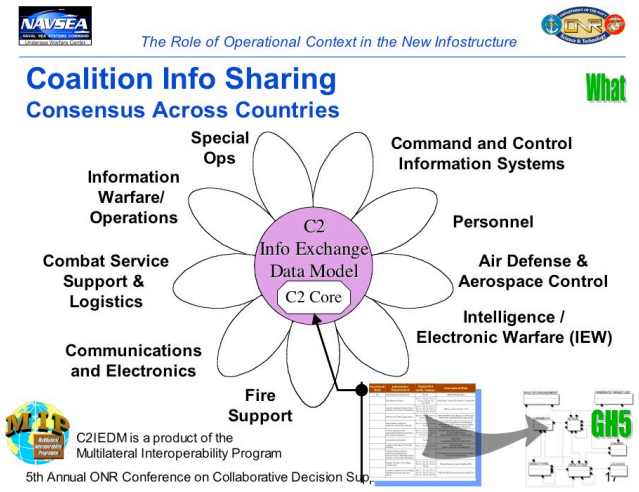
The liaison role defines general command and control information exchange needs. These can be related to Unified Joint Task List tasks and conceptual data types. This assessment describes what must be exchanged, not how or between which systems.

Within "Power to the Edge" it is asserted that classic system-to-system information exchange requirements (IERs) approach to interoperability is leading us down the wrong path because it discourages wide sharing information and pre-supposes what information each systems needs and from where it will come. Instead, Power to the Edge envisions each system putting information on the GIG where appropriate users can find it and exploit it. This is the approach we are describing here, describing the types of information that an organization consumes and produces.



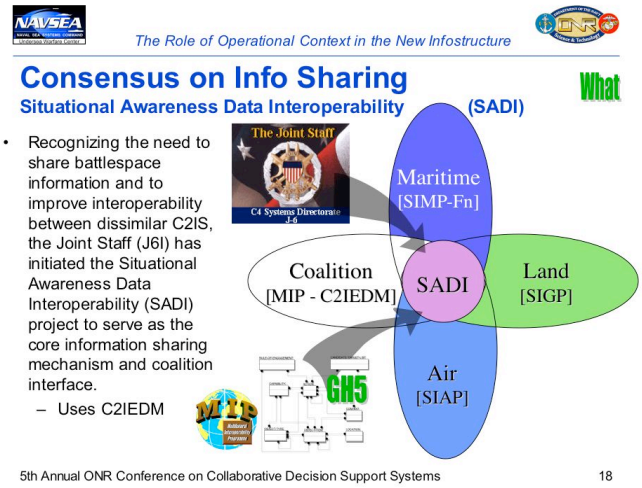
The core set of information that supports command and control relationships; tasking, status, etc., is common to any of these functional areas. It is not surprising that below the functional specifics we would find a command and control core. These functional and organization independent core set of informational exchange capabilities are at the center of GIG concepts and services - which are attempting to find the things that are common across the many functions,

players, etc. Please remember that we started with an operational consensus on command and control, and we are now recognizing how rich and widespread this consensus is and how it can be used to build a new technical paradigm supporting the GIG and providing power to the warfighter.



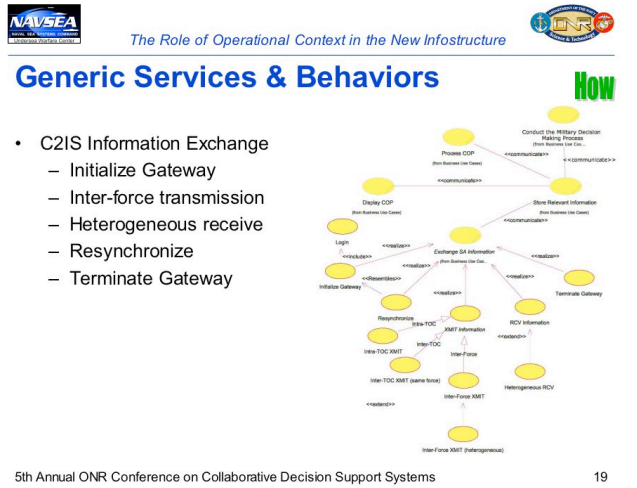
The core set of information elements we have been discussing are actually a subset of an even richer consensus that has been developed within, what is now referred to as, the Multilateral Inoperability Programme (MIP). MIP, composed of mostly but not exclusively of the NATO community, has been working to improve multinational Army interoperability from the operational to the tactical level. The operational consensus developed has been documented formally in what is now referred to as the C2 Information Exchange Data Model (C2IEDM). (Note it is also referred to as the Generic Hub version 5, or GH5). This operational consensus and the data model are endorsed by NATO. Remarkably, for ten years a group of international operational experts worked from the top-down considering, "What do we need to do? How do we do command and control? What are the kinds of information do we need to exchange?" Their scope of regard was across a wide range of functional areas, actually broader than is shown on this slide.

They defined a core generic military operations ontology, suitable for expanding to Joint operations. 20 Nations are now participating in this activity! The operational consensus serves as the basis for defining the battlespace, and the relationships between entities in the battlespace. This defines the information elements, and enables the creation of shared semantics and syntax. The resulting ontology, is a very important body of work because it has an international pedigree, is broad enough to serve as a core for Joint, it is extensible, it is system independent, and it demonstrates that the "one-to-many" approach is not only conceptually possible but is practical in an operational and technical environment of many dissimilar systems – in other words an important "cornerstone" for the GIG.



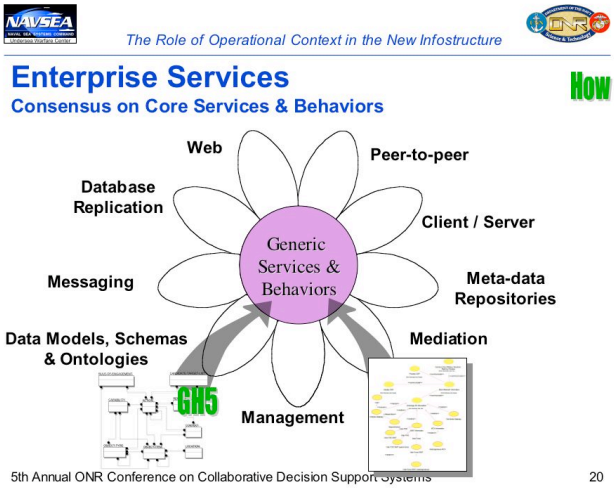
The Joint Staff has sponsored the "Situational Awareness Data Inoperability" project within the Family of Interoperable Operational Pictures (FIOP) effort to showcase the MIP capability here in the U.S. in a Joint context. SADI will use the MIP C2IEDM as its operational and technical baseline definition. SADI will implement an interface between the C2IEDM and GCCS. The MIP's international specification for sharing situational awareness information, or as I would refer to it "operational context", will only partially map to GCCS, because C2IEDM's ontology is considerably richer than that within GCCS.

So there is an emerging standard for how to share information and context about battlespace. In a GIG world, whatever system you're building, you will need to produce and consume information to a GIG representation standard – and that standard could, arguably should, be based on the MIP consensus. That said the MIP solution does not place any constraints on how a system represents the battlespace inside its own functional architecture or application software. Program managers can use whatever is appropriate for whatever reason. When their system connects to the GIG however there will be a system independent interface and a broader ontology that must be correctly addressed.

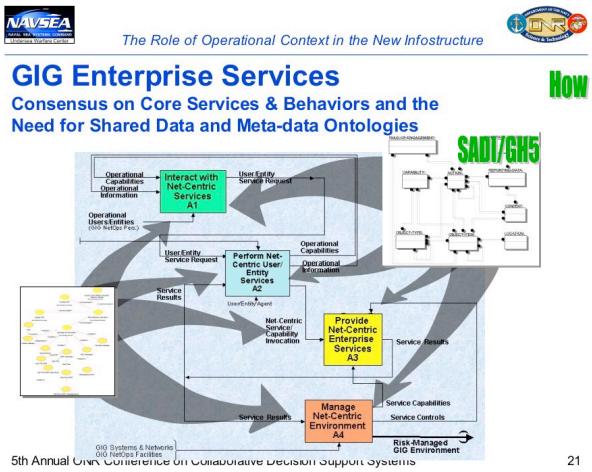


We started by considering the essentials for force coordination and derived through a consensus and system independent process a definition of the battlespace and how to represent it. Now that we have a shared and extensible representation we need to consider how we actually provide this information to the many warfighters that need it?

In a network environment information is often provided through a service that resides on a remote system. A user system connects to a service and typically requests information. When considering enterprise-level solutions it quickly becomes clear that it would be best if every different type of information or system didn't present a unique type of service or behavior. And in fact there are many generic and core services and behaviors that can be identified. These would for example enable a user or system to identify itself, establish a connection when authorized, update when required, and terminate a connection. These behaviors again require a consensus, this time at the technical level, of what a service is and how it and the client will behave. Without such a consensus it is likely that two systems will not interoperate. Conversely, the worldwide agreement on HTTP and HTML shows the power of consensus.



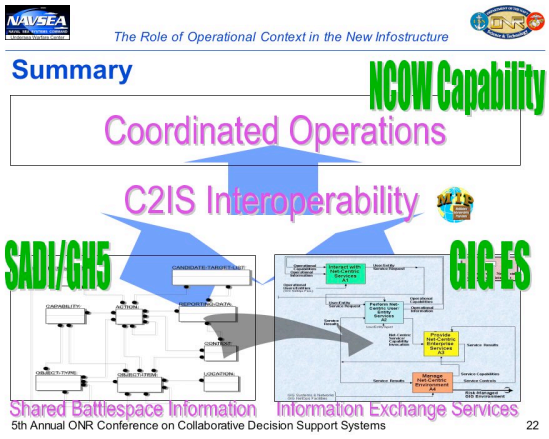
Within an enterprise when there is a shared ontology and a core set of generic information services there may still be multiple methods and requirements for how information is shared. This is a different version of the "one-to-many" requirement, specifically, that information is logically represented "once" but sharable in "many" formats. As an example, a unit position reported to the GIG might later show up as latitude-longitude coordinates on a chart and also text in a table. Or it might be presented on a web page or in a database replication event. Similarly, US Message Text Format (USMTF) format, C2IEDM format, or XML format should present alternative views of the same information. We need a common operational consensus and ontology to underlie both the information / context we must share and the different methods we will use to move the information to different users.



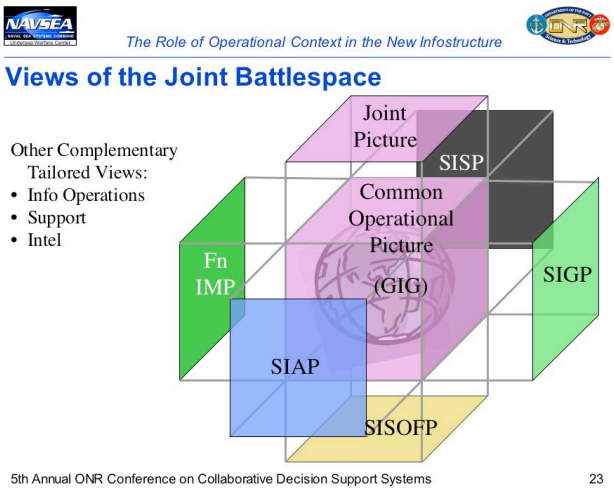
The ideas we have been discussing are relevant to the US efforts to define and implement GIG enterprise services. Each of the colored boxes in this slide represent a high-level characterization of core common services that will support warfighters and also manage the GIG. Note you see no systems here only services that all systems will be required to use and comply with. These services will control who has access and priority to which information and services. The GIG architecture plans recognize the importance of shared formal ontologies for information exchange and exploitation. SADI and C2IEDM have been identified as a GIG Key Interface Profile.

A common core extensible ontology for data and information is not sufficient. The GIG expects to use metadata to support rapid discovery, filtering, and organization of information on the GIG. There must be an operational consensus on what metadata is required, its semantics and syntax. How will this be produced? The great news is that "one man's data is another man's metadata", or more simply, the C2IEDM is also great baseline for defining metadata.

Discovery services on the GIG will need to be more than text string searches. C2IEDM-based metadata can be used to describe a rich operational context that can in turn be used by applications, decision support systems, and intelligent agents to discover and better interpret ongoing operations and events.



Let me summarize the ideas I have been presenting in the context of the consensus framework. We started with the need for an operational consensus on the nature of coordinated operation. In a practical sense it is through various interoperable C2IS systems that we attempt to share information and actually coordinate operations. The information to be shared must support the operational command and control process and consensus. The work of the MIP captures both in a manner that has led to demonstrated multinational capability. This same operational and technical consensus must be supported by GIG enterprise (and multinational, interagency) information exchange services. Thus, the MIP efforts will play a key role in defining the GIG and how Joint and Services systems interact with each other and with allies.



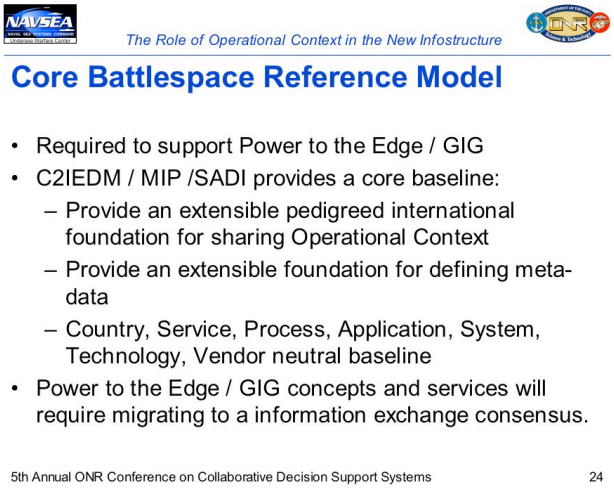
Consider for a moment that each commander requires a view of the battlespace appropriate to his or her role and responsibilities. The FIOP, the Family of Interoperable Operational Pictures effort is attempting to develop "pictures" of the battlespace tailored to various types of commanders. The hope is that by addressing the needs of commanders that the FIOP will deliver a "non-stovepipe" more integrated and tailored tactical picture to the warfighter. There are some that are concerned that FIOP will deliver new "stovepipes" because it is fundamentally working to integrate current systems in a "many-to-many" manner. If the maritime picture is built and maintained independent of the ground picture, and visa versa, then work is required to figure out if the two independent pictures/databases are actually aligned - this is part of the stovepipe problem.

"Power to the Edge" says put your information on the GIG. To return to our maritime / ground picture example, if the maritime commander and ground commanders both published to the GIG (the "purple cube" on the slide) then each can pull mission information from the GIG and view a Joint battlespace containing appropriate naval and land forces. Each commander posts what he knows and then any other warfighter can generate a tailored view by pulling info from the GIG. So on this slide the various FIOP "pictures" are instead being portrayed as "views" on the GIG common operational picture.

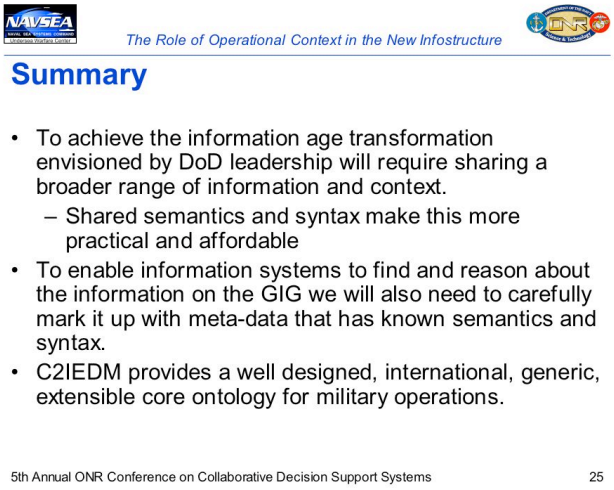
The notion of operational context is really at the heart of creating these views. This is because providing the right information, at the right time, to the right person is, I think, only practical

when one understands the operational context. If I want to know what information the maritime commander, or any of his organizations or systems needs one would first look at the operations order and review the maritime commander's operational and tactical responsibilities. This context defines what is relevant to the maritime commander. In the future agents and information systems will in fact be able to read this operational context, reason about it as people do today, and determine what is relevant and what should be in the view.

Note that there are other complementary tailored views such as information operations, intelligence, logistics, financial, etc.



The C2IEDM provides a core reference model that I believe enables many of the key ideas being advocated by "Power to the Edge". The great news is that it already exists. It is extensible, pedigreed, and really very well suited to sharing a broad set of operational context. It is suited to both the data and the metadata. It is country, Service, (as in Navy, Army, Air Force), process, application, system, technology, and vendor neutral! Thus, when you look at this data model it doesn't look like any particular system. It's much richer and more generic and for these reasons it is highly appropriate as a neutral representation for the GIG.



I will conclude by referring back the information age transformation that is envisioned by DoD leadership and my assessment that to accomplish it we must be able to share a broader range of information and context with the information systems that will assist us. Shared semantics and syntax for information and metadata are required to make this practical and affordable on the GIG. The work of the MIP and the international consensus that stands behind the C2IEDM provides a well-designed, international, generic, extensible core ontology and capability supporting military operations.

"Your talk brought to mind one of my favorite vocations which was England and the United States, two great countries separated by a common language, and in the context here it makes me wonder how close must the ontologies of different users be in order to interoperate? Is there some way of actually qualifying that or measuring it? And number two, how close produces fatal insidious errors? I mean it's nice to say we're gonna have, you know, a universal language, ontology, and meta-tags, but how do we measure that and how do we measure the potential harm when we don't exactly achieve that abstract goal?"

This could be a topic for a whole other presentation. I think a key idea here is that the ontologies need to be unambiguously mappable, one to another. For example, the system that you're working on needs to be able to pull information from the GIG, which I'll say is represented in C2IEDM ontology form. You need to be able to unambiguously map that to your system and its information space. If you can't do that then we don't have a consensus on things in the battlespace, how they are to be represented.

I'll give you an example: A couple of years ago I tied together two data fusion systems. Both allowed you to talk about the classification uncertainty associated with a track. In System A you could make a probabilistic kind of statement: I think this track is 60% probability sub, 30% probability airplane or surface ship, and 10% I don't know. In the second system you could say unknown surface, air or sub. Now both of those representations were perfectly reasonable to the engineers that built them. But they are not unambiguously mappable from one to the other. What does 60, 30, 10 become? Unknown? Submarine? I mean, you could come up with some business rules, but it just doesn't work in an unambiguous way.

Now, you're going have to make a case to me why we need these two ontologies that fundamentally aren't equivalent and aren't mappable. What's the value added in having two different representations of something that can't be cleanly mapped back and forth? If you want to use a broader extended ontology, fine. Each functional community can extend the common core and do it in such a way that the new elements link to the core. C2IEDM is about achieving interoperability written large, about describing the core.

And that's really the challenge, we need to share a common understanding the battlespace before we worry about working all the way down to the technical mappings. Technical syntax and semantics have to fit with the conceptual and broader set of ideas that need to be exchanged. Otherwise you're not effectively communicating or coordinating.

Reasoning about the Perception Using Software Agents

Presentation to the
ONR Workshop on Collaborative Decision-Support Systems

Dr. Mark Youngren
MITRE
(703) 883-6446 (MITRE)
E-Mail: youngren@mitre.org

LIMITED DISTRIBUTION: Distribution authorized to the Department of Defense and DoD contractors only: Software documentation 6 Jun 2002. Other requests will be referred to the JWARS office, OSD (PA&E)

Presentation Outline

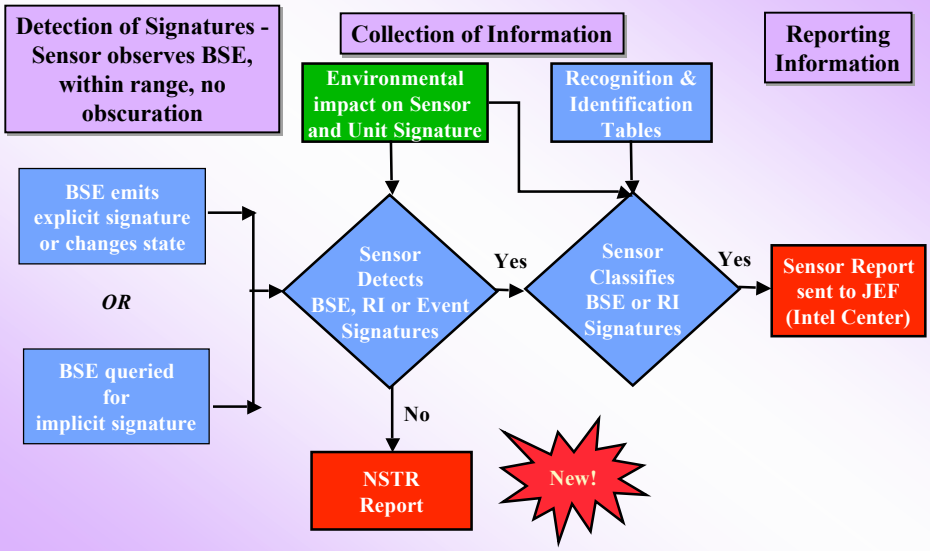
- Brief outline of process through which the Joint Warfare System (JWARS) model creates a perception or battlespace situation awareness (SA)
- Elements of a battlespace situation awareness
- Reports and information needed to develop a full SA
- Reasoning that can be made based on the full SA
- Development of a software agent
- Representing C2
- Summary

A Caveat

- The research discussed in this paper that will support the development of an SA agent has been in support of the JWARS office. However,
  - Not all of the research is completed. Not all of the research has been accepted as yet by the government and JWARS users groups for inclusion in the model, although all of the work submitted to date has been accepted
  - Not all of the research accepted and expanded into model design has been coded and included into the JWARS model
- Therefore, you will not see everything presented here appearing in the current (Beta release 1.4) version or the release under DT (ver. 1.5) of JWARS
- **This paper has not been approved by, nor does it necessarily reflect the views of, the Department of Defense, the JWARS office, or the MITRE Corporation. Viewpoints given in this presentation are attributable to the author only**
- This paper is being presented to suggest possibilities for how we think about and model perception in combat simulation models - or at least to spark some debate and other designs for perception

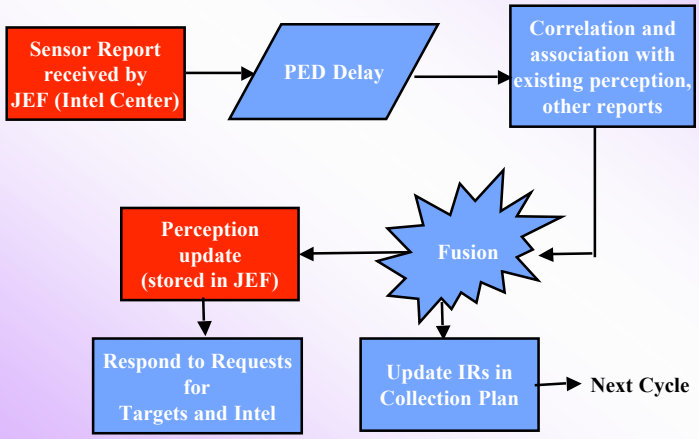
3

Sequence of Sensing



4

Sequence of Correlation, Association, and Fusion



5

JWARS - A Full, Complex Perception

JWARS will have a much richer, more complex perception as a basis upon which to reason:

- A unit-based list of perceived enemy (friendly, neutral, coalition, civilian)[1] units
  - Their attributes are maintained as *probability distributions* that are updated over time, not single averages or "most recent report"
  - **Fusion is actually modeled, not just assumed**. Thus there is a mathematical process that links C4ISR capabilities to unit perceptions.
  - Other attributes (location, activity, etc.) are also distributions
- A geographical data structure indicating amount & type of ISR effort directed at an area
  - This is used to develop the inference about where enemy units are *not*.
- Together, these allow us to infer enemy *intent*.

[1] This is not in the current code but is in the long-term design

6

Information used to Create a Battlespace Awareness in Combat Simulation Models

7

Information Typically Found in Combat Simulations – the "old" way

- Target-based reasoning is the traditional representation
  - Where are enemy units that I can strike? This requires a location, unit type, and characteristics of the activity / location (e.g., dug in)
  - Many simulations assume unit type and activity are known if a unit is detected, then the simulation focuses on target accuracy and timeliness
- Force Strength is the other traditional information structure
  - Force ratios are often used to decide whether to attack, defend or withdraw
  - Simple models use ground truth or average strength, often summed linearly based on unit assets and asset weights
- Both of these are in JWARS, but much more information is available even for these basic functions
  - A fundamental difference is that we constantly track and update the *uncertainty* about the "facts" that we perceive

8

Information that is not Unit Based

- Simulations have always defined their perception in terms of units acquired - only part of the information available and needed for reasoning
- Other information needed:
  - Unit activity *over time,* not just snap-shot based
  - Identifying over the entire battlespace where the enemy is and is not - as well as the types of units present
  - **Uncertainty** about this dual (unit and area based) perception
    - How old is the information?
    - How well have we classified asset types, activities, special units?
  - Friendly status, to include coalition forces
  - Status & presence of civilians, neutrals, "collateral avoidance areas," etc.
  - **Battlespace inference** - mines, obstacles, road conditions, bridges, etc.
  - Enemy ISR - what does the enemy likely know about friendly units?
  - **Enemy intent -** concept of operations, objectives, etc.

9

Reasoning about the Situation

10

Why do we Reason about the Situation?

- Traditional combat simulation information:
  - Targets for strike
  - Enemy unit locations
  - Strength of units in contact / near friendly units
- Traditional combat simulation reasoning:
  - Optimal or at least satisficing allocation of strike assets to targets
  - Attack/defend/withdraw decisions based on force ratios
- Other information & reasoning needed:
  - Collection management - where we place sensors depends on what we know and what we don't know
  - Enemy intent - to permit proactive combat operations and denial ops
  - Friendly Maneuver - depends on battlespace knowledge, enemy presence & absence across battlespace, enemy status, and enemy intent
  - Force Synchronization - depends on time sequence of previous activities

11

How Can We Do It?

Algorithms that permit an Agent to reason about the situation:

- MORSS 00: JWARS correlation, association, and fusion algorithms allow us to develop & update distributions of asset counts simultaneously over varying levels of classification
- MORSS 01: Likelihood functions based on sensor data & prior distributions allow us to infer enemy unit types and infer enemy force absence likelihood
- ICCRTS (Quebec Sept 02): Inference of enemy intent based on enemy unit types inferred and the inference of enemy absence used to develop likelihood functions over a sample space of possible enemy actions formed from IPB and the scenario
- Supporting algorithms & code: Clustering algorithms to aggregate units into forces; Collection management that accepts different ISR objectives; C2 knowledgebase "plug-ins"

12

Agent-Based Reasoning (1)

We intend to build an independent software agent that can reason about a situation based on a rich perception, to reason about:

- Synchronization – What is the status of friendly, enemy, and other forces in the area? Is it time to initiate the next phase, branch, or sequel to the operations plan? Do subordinate units need to be ordered to plan or to accomplish something?
- Intent – What is the enemy operational intent? How well is the enemy accomplishing his plan? What actions can be done to prevent his reaching his objectives?
- Collection Management – Where do we send sensors? Do we send sensors to areas where we know enemy are, to obtain better and more current information, or do we look in areas we haven't looked in for some time? What is the best plan overall?

13

Agent-Based Reasoning (2)

The software agent can also reason about:

- Hypothesis Generation & Planning – What are our set of hypotheses about the enemy intent? What are the hypotheses about the situation (location & activity of all forces)? Is it time to drop old prior information and treat new information as current (this is done when you think the underlying situation has changed)?
- Multi-source battlespace awareness – How do we employ multiple sensors to provide the best overall situation awareness? Are we getting evidence of deception, from different sensor types that provide different views? How can we fuse type and number information? How are situation and mission reports fused with ISR reports?

14

Why an Agent?

- "Agent based software" has become an overused buzzword. Nevertheless, there are uses of software agents that provide new capability.
- The proposed agent will be a software plug-in or federate (depending upon the main simulation code) that can independently evaluate sensor information and produce a battlespace awareness "report" and respond to queries about the current situation. The agent will also have a rule base to recommend decisions (C2 actions).
- An independent software object is reusable and adaptable to many simulations with less modification than an embedded block of code in a model.
- The agent algorithms can be copied even if the software is not reused, provided an adequate description of the algorithms exists.

15

What about C2?

- The representation of the Command and Control (C2) process in combat simulation models is probably the single most difficult challenge in modeling
- Many approaches have been suggested. Before you can choose between them, you need to decide
  - Is the C2 normative, prescriptive, or descriptive?
  - Do you use people, code, or both?
  - Do you represent uncertainty and variability in decisions as well as in decision inputs & outputs?
  - How will any choice affect an analysis?
- Before we can deal with C2 completely, we need to have a decent representation of what is known, as suggested in this paper

16

Summary

- The basic capability exists to combine previous research and algorithms into an independent software agent.
- The agent will incorporate state-of-the-art algorithms that can develop a battlespace awareness, make inferences about the situation, reason (make judgments) about that situation, and provide C2 rules that drive collection management and suggest courses of actions and hypotheses to the main C2 agent or process
- If the agent technology is accepted for use within the JWARS model, the agent will be a software plug-in for JWARS.
- The prototype federate will be made available for other model developers.

17

Conclusion

- Battlespace Awareness is far more than the digital equivalent of icons on a map
- The value of many improved sensor and processing capabilities will never be seen in exercises or models if we only model the process of accumulating more icons on the map
- The C2 is C4ISR is the next major challenge – but to reason, we must have a rich, complex set of facts and inferences to start with
  - This is equally as important for human commanders as it is for models of C2 in warfare
- The agent-based approach will allow us to independently test, share, and compare the capabilities of our perception inference among many modelers, testers, and analysts

18

Backups

19

A Perception is More than Icons on a Situation Map

Suppose we have an area in the perception without any perceived enemy units. Is this because

- We have searched the area and observed nothing, or
- We haven't been able to look in the area.

These have two very different impacts on the commander's decision, yet most models fail to distinguish between them

JWARS will model the process of searching an area and finding "nothing to report." It will also permit false alarms to occur in areas where there are no actual BSEs present.

This information is contained in a geographically-based data structure that can be used to infer the likelihood that enemy units are or are not present in specified areas.

20

Reasoning about the Perception Using Software Agents

Presentation to the
ONR Workshop on Collaborative Decision-Support Systems

Dr. Mark Youngren
MITRE
(703) 883-6446 (MITRE)
E-Mail: youngren@mitre.org

LIMITED DISTRIBUTION: Distribution authorized to the Department of Defense and DoD contractors only: Software documentation 6 Jun 2002. Other requests will be referred to the JWARS office, OSD (PA&E)

Ontology-Based Applications for Automating Decision Support

Dr. Steven P. Wartik, swartik@ida.org
Dr. Francisco Loaiza, floaiza@ida.org
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311

Abstract: The US Department of Defense has laid out tenets of *net-centricity* to help services and organizations utilize fused, web-based information. The DoD's chief information officer has identified ontologies as the means by which data will be made understandable in support of net-centricity. In this paper we explore how ontologies can contribute to the C2 domain. We present a C2 ontology we have created based on the Generic Hub information exchange data model. We discuss an agent-based tool we have implemented that uses the ontology to provide decision support capabilities. We also use our experiences to speculate on the strengths and limitations of ontologies in achieving net-centricity.

1 Introduction

Throughout history, the common complaint of decision-making warfighters has been lack of information. The absence of a common and complete operational picture has resulted in mishaps ranging from minor discomforts to the Light Brigade's infamous blunder. Making decisions that look reasonable in hindsight implies full situational awareness, something that has been sorely lacking for most of recorded history.

The DoD's *Global Information Grid* (GIG) is a significant step towards the ability to provide full situational awareness. The GIG, which aims to interconnect all warfighting data, is a major paradigm shift for the DoD. It is in part a recognition that the old strategy of centralized data administration across the entire department is impractical. There exist too many deeply entrenched cultures within DoD to create an atmosphere of fully seamless data exchanges among all domains. Data sharing cannot be mandated in such an environment. To put it another way, data cannot be "pushed" against someone's will.

DoD's new paradigm is to nurture individual *Communities of Interest* (CoIs). Each community will be responsible for identifying the set of data it manages. Each CoI will be encouraged, though not strictly required, to make its data visible on the GIG. The DoD believes this increased data visibility will better enable effective decision-making than the current environment. This paradigm is something of a double-edged sword. On the one hand, CoIs are under no obligation to make data visible, nor are they required to avoid duplicating existing data sources; this gives each CoI considerable freedom and flexibility. On the other hand, the existence of data from one CoI should discourage others from undertaking the effort of regenerating the same data over and over; this should encourage the growth of net-centricity.

To achieve net-centricity, DoD's Chief Information Officer has established seven goals.[1] The following is a summary of these goals:

[1] J. Stenbit, Department of Defense Net-Centric Data Strategy. May 9, 2003.
http://www.defenselink.mil/nii/org/cio/doc/ Net-Centric-Data-Strategy-2003-05-092.pdf

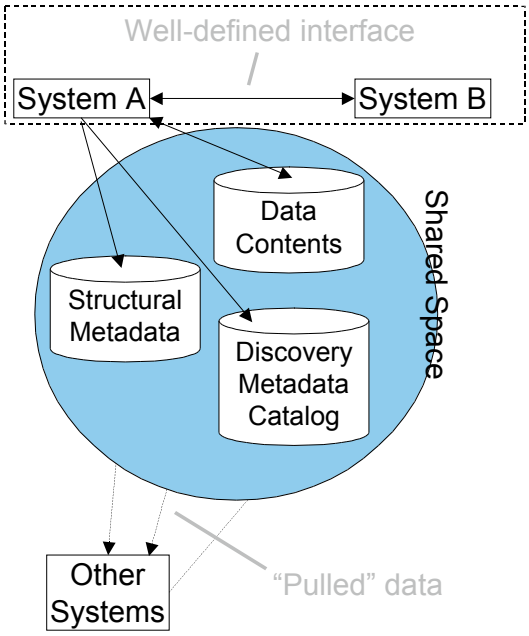


Figure 1. Net-Centric System Execution Concept

1. *Make data visible:* Users and applications must be able to discover the existence of data.
2. *Make data accessible:* There must exist shared spaces to which users and applications can post data.
3. *Institutionalize data management:* Approaches to managing data are incorporated into DoD processes and practices. Note that this goal covers only data management, not the data itself.
4. *Enable data to be understandable:* Users and applications must be able to comprehend data structure and semantics.
5. *Enable data to be trusted:* Users and applications must be able to determine and assess the degree to which they must trust each datum. In other words, attributes such as security and pedigree must be known.
6. *Support data interoperability:* Metadata must be available to allow mediation or translation of data between interfaces where necessary.
7. *Be responsive to user needs:* Approaches will evolve in response to user feedback.

Figure 1 shows how realizing these goals will achieve net-centricity. The area inside the dashed box denotes a single CoI. Within this area, all systems communicate using well-defined interfaces. This is possible because the CoI can exert control over the systems it defines, mandating standards as it sees fit. Problems traditionally come when Other Systems outside the CoI want access to the data provided by System A or System B. With no control over the format or content of that data, these Other Systems are likely to incur risk.

Net-centricity aims to reduce this risk. Systems A and B are still free to communicate through their well-defined interfaces. However, they are also encouraged to publish their data to a shared space. This shared space contains not just the data (Data Contents) but also information that can help other systems discover if the data meets their needs (Discovery Metadata Catalog) and information on how to interpret the data (Structural Metadata). Rather than creating fixed

interfaces, other systems may dynamically search for data – i.e., browse through the discovery metadata catalogs in a known set of shared spaces – and choose the set that best fits their current situation.

This is an excellent scenario for improving decision support applications. A decision support system can continually search the GIG for whatever data is most appropriate, from information on the next town to prospects for resupply from halfway across the globe.

By the same token, it is also a scenario for *information overload*. The prospect of a decision support system finding, and forcing a warfighter to sort through, too much relevant information is real and worrisome. Net-centricity must ensure that the warfighter has access to not just the right information but the right amount of information.

The DoD has addressed this issue in its goal of making data understandable. Understandability means more than structural and semantic descriptions. It implies an ability to determine the value of data. An application that is pulling data must be able to filter the data based on perceived need.

The net-centric strategy identifies CoI-specific *ontologies* as one facet of making data understandable. Ontology building is generally understood to be a technique for syntactic and semantic understanding of data. Examples of what an ontology encompasses include data categorization schemes, thesauri, vocabularies, and taxonomies. An ontology would describe the data of a CoI in ways that promote use of that data by systems in other CoI's.

To be useful in a net-centric environment, an ontology must be formal and executable. System developers have often employed ontologies informally as part of system documentation (e.g., drawings of data models), which may suffice for a human reading that document but of no use to a decision support software application. The premise of an ontology in the net-centric data strategy is that other systems can access it to determine whether the data it describes is useful or not.

Figure 2 shows how an ontology is used. Each CoI will develop and maintain ontologies of its data, and register those ontologies in the DoD Metadata Registry. Other systems search these global registries when they need information. The Registry both describes the type of information (the details are in the structural metadata catalog) and the shared space in which to find it. Other systems use registries to identify likely data sources, then use the contents of the Shared Space to retrieve data and determine its meaning from the ontology.[2]

The power of ontologies, then, will stem from their ability to promote dynamic access to data. Applications will no longer be constrained by a fixed set of interfaces. Each time they desire information, they can search as broadly – or as narrowly – as is appropriate to their context.

The underlying assumption is that ontologies will be sufficiently expressive to let applications determine the relevance of data. Generally speaking an ontology is a specification of data structure and semantics. In order to support the net-centric goals an ontology will have to be written using a formal language that is not only understandable to humans but also machine-processable. When that is the case an application looking for some type of data ought to be able to use an ontology to determine whether a CoI offers that data; whether or not it is somehow

[2] We use terminology loosely here. Strictly speaking, an analyst identifies concepts (i.e., abstractions), which he then expresses in some ontology language; the result is an ontology. The data are concrete

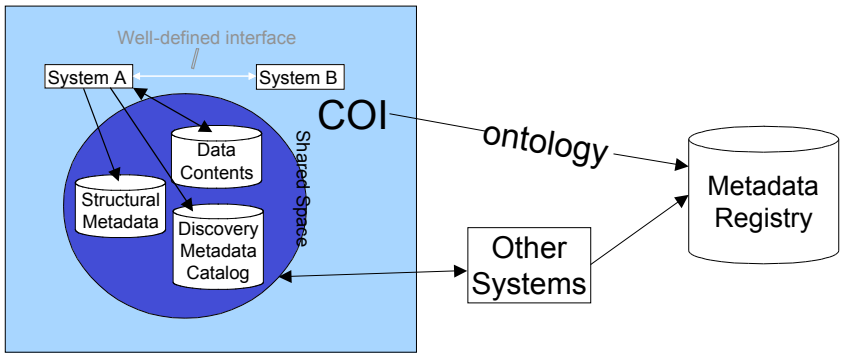


Figure 2. Use of Ontologies

better (e.g., more trustworthy) than equivalent data from another CoI; whether it is in a form that will be useful; and how it can be retrieved. No general-purpose solutions exist to all these problems.

2 An Exploratory Project

We have undertaken an exploration of how to use ontologies in a net-centric environment. Essentially, our objective is to explore whether the aforementioned assumption is valid. We are doing so by:

1. *Creating an ontology for the domain of command and control (C2).* C2 is a domain with a long, important history in warfare, and constitutes an area for which a CoI will likely exist either at the Service level or at the Joint level for all of DoD.
2. *Defining explicitly selected C2 concepts.* Modeling the entire C2 domain requires resources beyond the scope of a preliminary study. However, we have focused on concepts widely agreed to be necessary in C2. Our goal is to create formal statements of those concepts in the ontology. We have selected two concepts: *threats* and *operational readiness*.
3. *Evaluating the ontology using a prototype system of agent-based software applications.* We demonstrate that the ontology can be used as per the tenets of net-centricity.

This paper describes our progress to date.

3 A C2 Ontology

As mentioned above, ontologies need to be formal to, among other things, minimize ambiguity and enable machine processability. Formality implies rigorously defined structures and semantics. Extensive work in the area of formalization of C2 structures and semantics has been accomplished in the data layer specifications for information exchanges among C2 databases. Therefore, rather than to reinvent these C2 concepts we have chosen to base our C2 ontology on a preexisting formal C2 data model specifically designed to support information exchanges in a coalition environment. This C2 data model is the Generic Hub Information Exchange Data Model (IEDM), version 5 (hereafter referred to as GH5).

The GH5 is the NATO standard IEDM for joint and coalition operations. It has also been adopted by the Army's Future Combat Systems (FCS) program, and has been used at the Naval

instances of the abstractions. The data in the context of the ontology is properly termed a *knowledge base.* We use the terms "knowledge base" and "ontology" interchangeably in this paper.

Postgraduate School and the Naval Undersea Warfare Center (NUWC) for various data interoperability projects.

Figure 3 shows, using an entity-relationship diagram, the major elements of the GH5 that play a role in this paper. The GH5 models battlefield objects. Each instance of a battlefield object is modeled as an ObjectItem. There are five kinds of battlefield objects: Facility, Feature, Materiel, Person, and Organisation. An ObjectItem has one or more types. A type is modeled as an instance of ObjectType, which is a supertype of five kinds of battlefield object types that correspond to the different types of battlefield objects, i.e., FacilityType, FeatureType, MaterielType, PersonType, and OrganisationType.

Each of the type entities has attributes (not shown) that further categorize the type as one of a set of enumerated elements. For example, a PersonType may be DETNEE (a detainee, i.e., a person in custody), GOVEMP (a government employee), JRNLST (a journalist), or any of nineteen other values. Instances are not mutually exclusive. The GH5 would model a journalist in custody as an instance of Person associated with two instances of PersonType, the first with an attribute value of JRNLST and the second with a value of DETNEE.

The holdings relationship shows the association between an ObjectItem and the ObjectTypes it possesses. One attribute of holdings is the quantity held. For example, that a battalion holds a certain quantity of ammunition is modeled by an association between the instance of Organisation modeling the battalion and the instance of MaterielType modeling that kind of ammunition; the quantity is captured as an attribute of the instance of the holdings relationship. (The GH5 can also model associations between instances of ObjectItem; a battalion can, if it wishes, track every individual bullet. Such detail is seldom worth the effort, however, and Figure 3 does not show the GH5 elements for modeling it.)

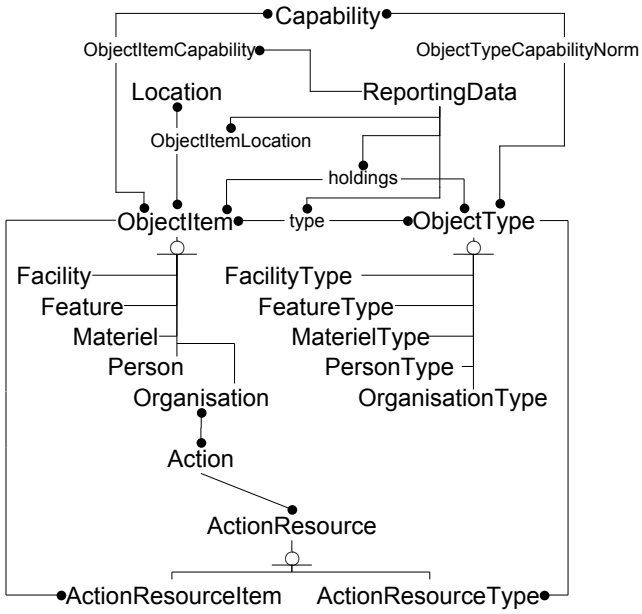


Figure 3. Entity-Relationship Model of Selected GH5 Elements

The potential abilities and effects of each battlefield object, and each battlefield object type, are described as a set of Capability instances. Each Capability instance denotes some physical ability or effect; the GH5 enumerates a standard set. There are capabilities that describe storage, mobility,

surveillance, firepower, mission, and engineering abilities. An ObjectType has a nominal set of capabilities. An ObjectItem has an actual set of capabilities.

A battlefield object has a location. The GH5 models location as an association between ObjectItem and Location.

With one exception, all the relationships discussed so far have a relationship to ReportingData. ReportingData is a central element of the GH5. Its attributes provide for time-ordered specifications. For example, the location of an instance of ObjectItem over time is modeled as a set of relationships between that instance of ObjectItem and a set of instances of Location. Each ObjectItemLocation has an associated ReportingData stating the time for which the relationship is valid, i.e., the time when the ObjectItem was reported to be at a Location. Similarly, each ObjectItemCapability relationship has an associated ReportingData instance stating the time when the ObjectItem was observed to have the stated Capability. But there is no ReportingData associated with an ObjectTypeCapabilityNorm. ObjectTypeCapabilityNorm describes nominal, not observed, capability.

The GH5 can model planned and actual occurrences of events. These are modeled as instances of Action. An Action can be associated with an Organisation. The relationship between the two describes the role of the Organisation with respect to the Action (approves, controls, initiates, etc.). An Action consumes resources. These may be specified either as resource types or as actual items, depending (usually) on whether or not the Action is a template. Similarly, an Action has objectives. These also may be specified either as resource types or as actual items.

3.1 Creating a GH Ontology

The ontologies currently being explored in government research institutions, as well as industry are expected to support basic reasoning tasks by allowing users and applications to draw inferences about data. The GH5 is an IEDM, and as such provides a suitable point of departure for an ontology; however, as a data model it lacks formal inference capabilities expected of an ontology, even though it has many implicit business rules that when formalized could support inferencing. For example:

1. *Its naming conventions do not map unambiguously to unique data types.* The GH5 has attributes whose names end with "quantity" that, as expected, describe some quantity. Their values, however, are not interchangeable. The attribute airfield-hangar-area-quantity defined as: *The two-dimensional measurement that represents the total hangar area (in square meters) in a specific AIRFIELD*, is measured in square meters. The attribute bridge-span-quantity, defined as: *The non-monetary numeric value that represents the number of sections that a specific BRIDGE may have*, is a unitless integer. One cannot, therefore, make any generic assumptions on the units of measurement used based only on the class word at the end of the GH5 attributes.
2. *It does not formalize measurement concepts.* The fact that in GH5 airfield-hangar-area-quantity measures area in square meters is expressed in natural language. An ontology should express this formally so that applications can reason on that basis.

In our prototype we have used the Knowledge Interchange Format (KIF) as the basis for creating a GH ontology. In the KIF, knowledge is modeled as a set of *frames*. The KIF includes several kinds of frames, including *instances*, *classes*, and *slots*.

We model each GH5 entity as a class. The KIF includes subclass relationships between classes, and we take advantage of these where the GH5 uses subtypes. Thus our ontology has an ObjectItem class, with subclasses Facility, Feature, etc.

We model GH5 attributes and relationships as slots. An attribute is a slot of single cardinality. A relationship is a slot of multiple cardinality. KIF classes inherit slots. Thus the Facility class inherits all slots of ObjectItem.

Many GH5 attributes have as their domain a set of enumerated values. These values give meaning to attributes; the meaning is standardized across the C2 domain. When defining a slot for such attributes, we give the slot the same standard set of values. We are often able to use these values to help in inferencing. For example, the Capability class has a unitOfMeasurement slot. We can use its value to convert between two Capability instances.

We have also noted conceptually related GH5 attributes, and incorporated knowledge thereof into our GH ontology. Both ObjectItemCapability and ObjectTypeCapabilityNorm have a quantity slot. These slots model the same concept and can be compared to determine whether an ObjectItem is at, above, or below its nominal capability. We also note the distinction between slots that model different concepts, even if they are expressed in the same units. For instance, the class that models equipment type has slots stating height, length, and width. These slots are all of the same data type, but they are not semantically interchangeable.

We can also state relationships between slots that are implicit in the GH5. The Airfield class has a hangarArea slot; an AircraftType has length and width slots. We can use these slots to calculate the maximum storage capacity of an Airfield instance for a given AircraftType.

We do not need to model all GH5 attributes. In a relational database a substantial number of attributes are defined for the sole purpose of distinguishing between instances in tables and enabling their unambiguous, creation, retrieval, update and deletion. In the KIF, each instance is uniquely identified as a frame. Thus we omit all GH5 attributes that model keys.

3.2 Creating a C2 Ontology

The GH5 models individual entities relevant to C2, such as classes of materiel and actions. The GH ontology we have created is an adaptation of the GH5. It is still not properly a C2 ontology, because it does not model concepts relevant to command and control. These concepts are based on the entities in the GH5, but are at a somewhat higher level of abstraction. An example would be a threat. The concept of threat is central to C2; understanding what threats one faces is necessary to determine one's course of action. Thus a C2 ontology should explicitly include Threat.

The GH5 does not directly model threats. It models battlefield objects, which are the entities that can pose threats. It also models information about battlefield objects that can help determine if a given object poses a threat. For instance, the threat posed by a unit could be based on the unit's last known location, direction of motion, and types of weapons held. This is only one definition of threat, of course, and may not be proper for a given situation; but the important thing to realize here is that the GH5 possesses this information, and it can help in threat determination and evaluation.

We base our C2 ontology on the GH ontology, essentially creating a wrapper around the GH ontology as shown in Figure 4. We select certain C2 concepts – in Figure 4, threats and operational readiness – and define them in terms of information in the GH ontology. Figure 4

shows the proposed scenario for using the C2 ontology. It presupposes the existence of a GH5 database, i.e., a DMBS that implements the GH5 IEDM. This database receives information both from a network (i.e., the GIG) and from on-site observers. Information is first taken from the GH5 database and translated into the GH ontology. The C2 ontology understands how to access this ontology to translate entity-level information into C2 concepts. Decision support systems access the C2 ontology, which in turn accesses the GH ontology, to obtain information that aids commanders in decision making.

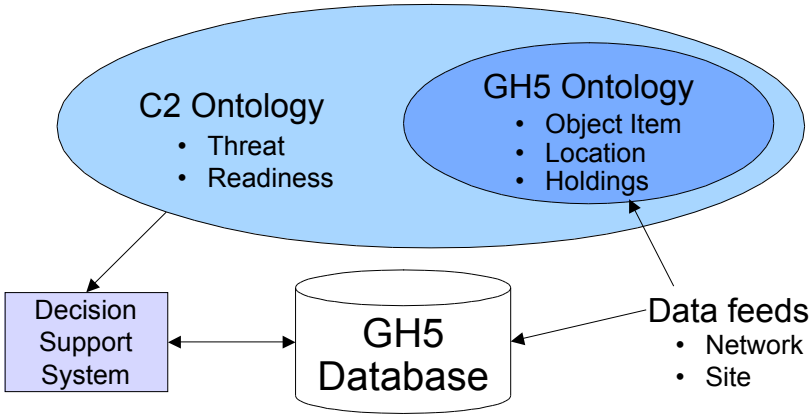


Figure 4. Scenario for Using the C2 Ontology

3.3 Implementing the Ontologies

We previously stated that an ontology must be executable, i.e., that its contents be interpretable and accessible to computer applications. Fortunately, several programs that model KIF-based ontologies are available.

We had several practical requirements for the ontology technology that helped us narrow our selection:

1. *The technology should be freeware.* This is an exploratory project, and we hope to distribute its results freely. This would be difficult with licensed software.
2. *The technology should run on multiple platforms.* Because of our distribution goals, we did not want to limit ourselves to a single environment, even one as widely used as WinTel.
3. *The technology should be useful on knowledge bases of realistic sizes.* We were not interested in creating toy examples that do not scale up; we wanted a convincing demonstration that ontologies could be used in real-world situations.

After some study, we settled on Protégé-2000.[3] Protégé-2000 is an open-source ontology- and knowledge-base editor written in the Java programming language. Its creators have evaluated its performance and found that it does not degrade until the knowledge base comprises on the order of 10^6 frames. This number may be too small once the GIG is fully realized, but we believe that for now it will suffice. We give some numbers below to justify this belief.

The GH ontology we have implemented is almost complete, meaning that it captures almost all of the entities, attributes, and relationships present in the GH5. Unfortunately, the GH5 is still

[3] http://www.protege.edu/

evolving, and we have not yet incorporated everything from the latest version (the expected release date of GH version 6 is November 2003). We have, however, included all the major model elements.

The C2 ontology is still in a rudimentary form. Our goal is to select a few C2 concepts and implement them as carefully as possible to test the realism that an ontology can offer. As such, we do not intend to create a complete C2 ontology. To date we have focused solely on threats; in other words, our C2 ontology consists of the GH ontology plus a single extra class, Threat, with slots that denote the threatener, threatenee, reporting organization, and perceived degree of threat.

Some metrics may help give a feel for the complexity of the C2 ontology. It has:

- 887 classes
- 633 slots
- 7,856 instances (most of which are coded domains from the GH5 specifications)

In other words, the number of frames is on the order of 10^4, 2 orders of magnitude less than that which would cause degradations in Protégé-2000's performance. We also have obtained some sample data, taken from a NATO exercise; it can be modeled using approximately 20,000 frames. This suggests that Protégé-2000 can handle real data sets.

4 Using the Ontologies for Decision Support

The next issue we considered in the project was how the C2 and GH ontologies can be most effectively used for decision support. The objective of net-centric warfare is to give decision makers access to the wealth of information available on the GIG. Of course, decision makers are not expected to search the GIG themselves; that would be far too time-consuming. Nor are applications supposed to push data onto decision makers, as that scenario would be arbitrary and overwhelming.

The alternative is for local applications to serve decision makers by continuously looking for, and analyzing, information the applications deem relevant. These applications are known as *knowledge agents*. The objective of knowledge agents is both to reduce the need for routine human operator intervention – e.g., to search the GIG in lieu of human subordinates – and to identify the best data to pull from the GIG for analysis and inspection. In a C2 scenario, knowledge agents would base their search criteria on factors such as current mission, current location, operational readiness, and perceived threats.

4.1 System Architecture

Figure 5 shows the general agent-based model we have adopted. Parallelograms represent knowledge agents. In this picture, there are three, each of which accesses the C2 ontology to perform analyses; as in Figure 4, the C2 ontology is a wrapper around a GH ontology, which obtains data from a GH5 database. One agent is responsible for threat perception. It analyzes the ontology to find conditions that indicate one organization threatens another. If it finds a threat, it notifies a threat response agent. The threat response agent analyzes the ontology to determine valid courses of action in response to a threat. These courses of action are formulated as GH5 actions, with resources appropriate to the action. The threat response agent prioritizes courses of action based on factors such as current mission and resource availability.

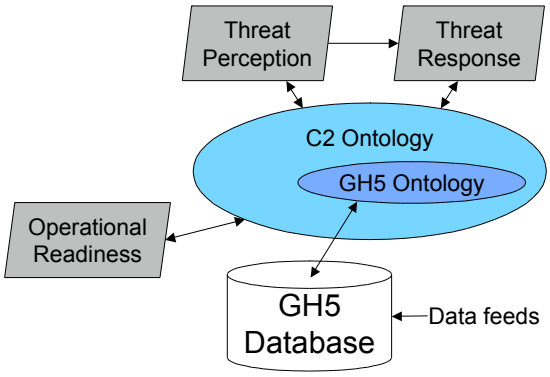


Figure 5. Software Agents and the C2 Ontology

The third agent is the operational readiness agent. Like the threat response agent, the operational readiness agent continuously examines the ontology to determine the perceived readiness of some battlefield object.

The purpose of an agent is not to make decisions but to assist decision makers by providing them with the information necessary to help them make said decisions. We envision this being accomplished through applications that interact with the agents. These interactions should be in a form familiar to the user. Figures 6–8 show the concept. A decision maker is using an application that presents a battlefield map showing the location of his and other units, both friendly (blue) and hostile (red). This application obtains operational readiness (the table in the lower left) and threats (the box on the right) from the operational readiness and threat perception agents.

At the same time, the application can display another window in the upper right showing the threat response agent's analysis of how the threat might be handled. Note that the decision maker is being given data of two types. The first type is simply informational: he is being informed of readiness and threat existence. The second type requires a response: he is being asked to select a course of action and make a decision. In both cases, the commander is still in control. The agents have simply pushed useful information at him, rather than forcing choices.

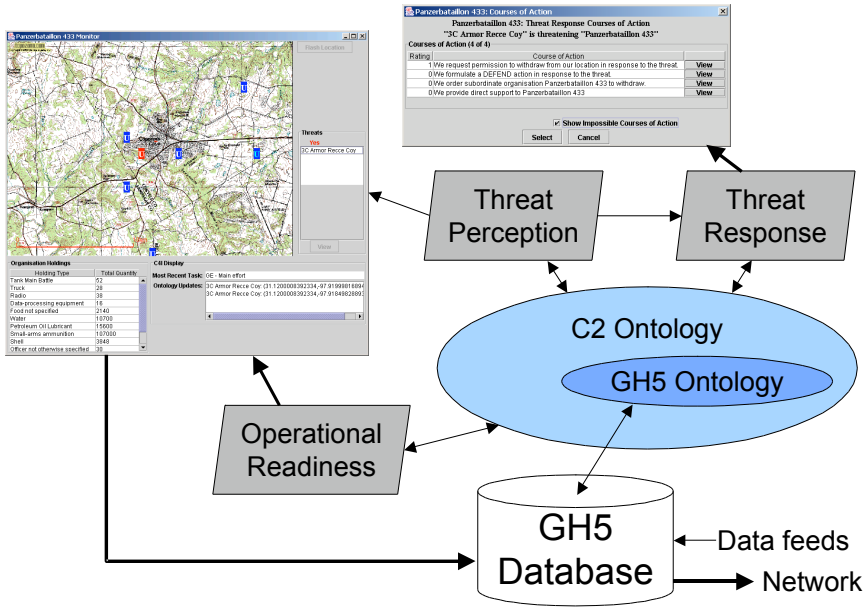


Figure 6. Decision Support Applications Using Software Agents

4.2 Implementing the System

We tested our ideas by implementing a prototype system based on the architecture described in the preceding section. Our objectives for this system were similar to those for the ontology: we wanted distributability, portability, and reasonable speed. Given that our knowledge base tool was written in Java, it made sense to find an agent-based framework written in Java as well.

We ultimately decided to use the FIPA-OS system. FIPA-OS is a Java-based implementation of certain standards created by the Foundation for Intelligent Physical Agents (FIPA).[4] It provides an architecture for running agents, and standardizes many of the languages and protocols needed for inter-agent communication.

We implemented the database using Oracle's Personal DBMS, a version of Oracle's DBMS software that is available for use so long as one does not use it to construct commercial applications. Personal DBMS comes with Java Database Connectivity (JDBC) software; we therefore can use it to store and retrieve GH5 data from our Java-implemented agents and ontologies. The use of a real DBMS brings our environment closer to a production level system.

As of this writing we have implemented the threat perception and threat response agents. We have not yet implemented the operational readiness agent. The system consists of approximately 17,000 lines of Java and 1,000 lines of other languages that are translated into Java.

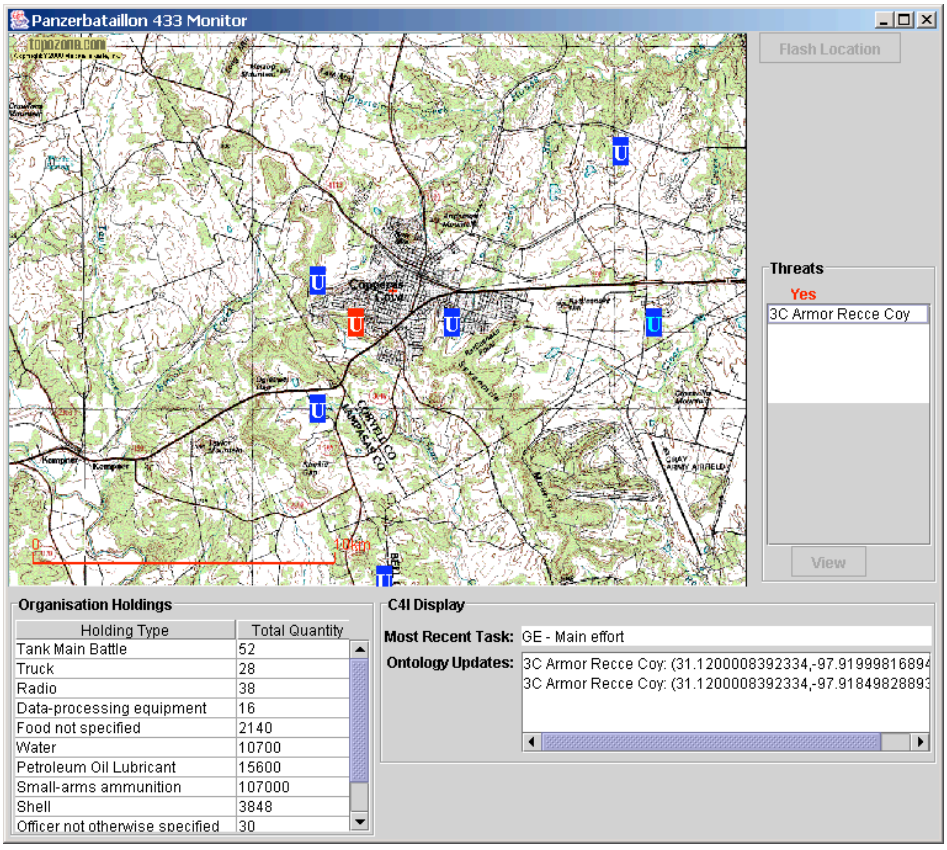


Figure 7. Decision Support Application (Detail)

[4] http://www.fipa.org

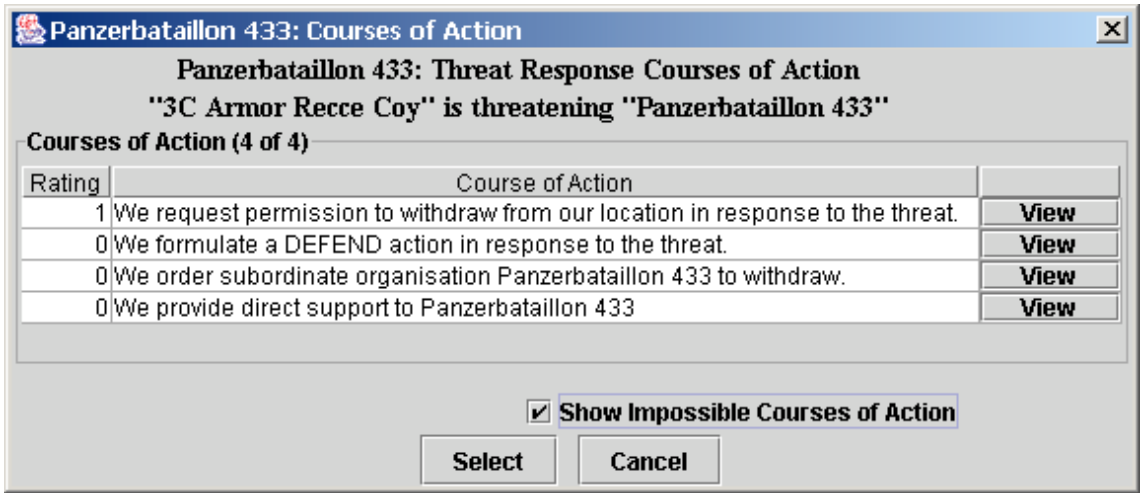


Figure 8. Threat Response Courses of Action (Detail)

5 Conclusions and Observations

Our objective in this project has been to test the net-centric data strategy's goal of making data understandable. We have concentrated on creating an ontology that would support the C2 community of interest. Creating an ontology is not the only aspect of making data understandable; one must also provide descriptors for the ontology that will allow agents to identify it on the GIG. However, an ontology is a necessary first step. [5]

The GH ontology we have created is structurally very similar to the GH5 IEDM. Each class in the GH5 IEDM maps to a class in the GH ontology; each organic attribute of the GH5 IEDM maps to a slot in the GH ontology; and each relationship in the GH5 IEDM maps to a slot in the GH ontology. This is partly a reflection of the capabilities provided by Protégé-2000; for instance, if Protégé-2000 supported many-to-many relationships instead of one-to-many relationships, we might have designed the GH ontology differently.

The GH ontology is an improvement over the GH5 IEDM in several significant ways. It explicitly identifies domains for each slot, thereby identifying which slots model equivalent concepts. It also identifies which slots model some physical concept, and in particular which model physically measurable concepts; with regard to the latter, it includes enough information to allow conversion between slots that differ in units. This notion of explicitly identifying concepts should prove useful when we need to create descriptors.

We also anticipate that the GH ontology can, in time, be extended with additional business rules that describe constraints. These will come from expert knowledge of how the enumerated domains used in the GH5 are applied. For example, the value AMPH of the GH5 attribute action-task-category-code means "To mount an operation launched from the sea by naval and land forces against a hostile, or potentially hostile shore." Mounting a sea-launched operation implies the presence of ships or boats, so any ActionTask with this category code must include ships or boats

[5] We are aware of the evolving *DoD Discovery Metadata Specifications* (DDMS) and plan to incorporate in later releases of our C2 ontology pertinent portions of that specification.

as an ActionResource. Individual applications can incorporate this kind of knowledge, but centralizing it in an ontology is much more useful.

In developing the C2 ontology we have realized that the rules needed to support threat analyses using the GH5 concepts can be quite complex. For example, our preliminary attempt using Protégé Axiom Language (PAL) to define the concept of a potential threat in the C2 ontology requires us to refer to substantial number of frames and slots:

```
(defrange ?status :FRAME ObjectItemStatus has-ObjectItemStatus)
(defrange ?hc :FRAME DS145_obj_item_stat_hstly_code)
(defrange ?hce :FRAME DS145_obj_item_stat_hstly_code-Elements)
(defrange ?statp :FRAME ObjectItemStatus has-ObjectItemStatus)
(defrange ?rd :FRAME ReportingData)(defrange ?rdp :FRAME ReportingData)
(defrange ?dt :FRAME Date-Type)(defrange ?dtp :FRAME Date-Type)
(defrange ?tm :FRAME Time-Type)(defrange ?tmp :FRAME Time-Type)
(exists ?status
  (and (has-ObjectItemStatus ?threatening-organisation ?status)
    (exists ?hc (and (hostilityCode ?status ?hc)
      (exists ?hce (and (type-instance-value ?hc ?hce)
        (enumerated-element-label ?hce "HO")
          (exists ?rd (and (provides-applicable-information-for-ObjectItemStatus ?rd ?status)
          (not (exists ?statp (and (has-ObjectItemStatus ?org ?statp)
            (exists ?rdp (and (provides-applicable-information-for-ObjectItemStatus ?rdp ?statp)
              (exists ?dt (and (reportingDate ?rd ?dt)
                (exists ?tm (and (reportingTime ?rd ?tm)
                  (exists ?dtp (and (reportingDate ?rdp ?dtp)
                    (exists ?tmp (and (reportingTime ?rdp ?tmp)
                      (=> (= ?dt ?dtp) (> ?tmp ?tm))
                        (> ?dtp ?dt))))))))))))))))))))
```

Clearly, there is considerable real-world work remaining. This too is partly a Protégé-2000 issue. We believe that future versions of Protégé-2000 incorporating a more powerful constraint language (e.g., OWL-Full), will probably go a long way in making these statements simpler to write and to process.

We have found FIPA-OS to be a suitable, although perhaps not the most sophisticated, platform for our agent-based implementations. More advanced platforms exist for developing agents, but they are usually tailored to a specific domain. Much agent research comes from interest in conducting monetary negotiations over the world-wide-web; this research is suited to electronic transactions but not necessarily to warfare. We have therefore implemented our own protocols as necessary, and we expect that future research will have to be devoted to this subject.

A Web-Centric Preference Acquisition and Decision Support System Employing Decision Times to Express Relative Preferences

Professor Jerald L. Feinstein, Ph.D.
The George Washington University
Monroe Hall, 21st and G Streets, NW
Washington, DC 20052

INTRODUCTION

This paper presents the general ideas of a new technique employing decision times to express relative preferences or degrees of confidence with respect to decision alternatives operating within a web-centric preference acquisition and decision support system. This is an alternative, neural net-motivated method employing decision times or reaction time metrics and a set of decision analytic techniques for capturing, synthesizing, and analyzing decisions, opinions, confidence, and preferences from subject matter experts as well as from the general population.

The paper's first part describes a sensory sampling methodology for transforming the time it takes to make a decision among a number of choices, two-at-a-time, into a set of ratio scaled relative preference, confidence, and decision consistency metrics using a modified Analytical Hierarchy Process (AHP) approach.

The second section describes a method for synthesizing individual results into a group decision metric, and for assessing the stability of that decision, where stability is the propensity of an individual or group to "change its mind" and defect to alternative choices.

BACKGROUND

The inability of a multiplicity of teams within large organizations to make the right critical decisions, at the right times, and in the right places, is now receiving renewed interest and much needed attention within the Department of Defense, the federal establishment, and in many private sector organizations as well.

According to Peter Drucker, eighty percent of all new products or services fail within six months or fall significantly short of forecasted profits. Thus, something appears to be very wrong with methodologies used in market research decision making concerning people's preferences for products. Is decision making in the Department of Defense, the federal establishment, or the private sector any better?

Lame excuses that challenges and complexities have grown beyond human scale, that available information is often conflicting and ambiguous, or that classic methods do not reflect how decisions are really made can no longer be tolerated due to the enormous and often tragic costs engendered by making decisions that are not only wrong, but not even close.

Decisions are about making choices among alternatives and combining objective, as well as highly subjective, information with individual and group expertise. Thus, major decisions in complex organizations involve integrating vast information resources with many choices among a large number of people. For any complex decision, it is crucial to know if it is a stable one. That is, what is the potential for individuals, or groups, to switch, back and forth, or oscillate among different alternatives? How confident are the individuals in the final decision, or to what degree is the selected alternative preferred to all others? How consistent are individuals or groups in making their decisions among possible alternatives? The real question is how to address the above challenges in complex organizations with real world constraints in order to assist decision makers in crafting better and more understandable decisions.

For example, military exercises often contain a Test and Evaluation component requiring the use of subject matter experts to evaluate and analyze results. It has been found, repeatedly, that the experts' assessments are often exceedingly subjective, with recommendations that are highly sensitive to change, and are strongly linked to the vagaries as to how the subject matter experts were selected. Often, the experts, themselves, express severe dissatisfaction with the decision process itself. In this paper, the challenges are discussed as well as the degree to which the alternative decision time or response latency methodology addresses the problems.

To further complicate the situation, conscious processes are involved when deciding on relative levels of preference or confidence among possible decisions, and these processes are known to be vulnerable to manipulation. Individuals sometime respond to the need for a decision in a manner that they think pleases someone, or respond in ways that tend to maintain a positive image.

In my interviews with subject matter experts and decision makers working within large military and private sector organizations, I discovered that several very real threats to effective decision making were obvious to these people. They knew very well why bad decisions happened in their organizations. They claimed it had to do with the organizational context in which they worked. Reasons provided were that their organizations were dedicated to textbook approaches to decision making that were heavy on the mathematics but not very good at coming up with the right decisions. These techniques often neglected the highly qualitative aspects of decision making and had very few mechanisms for incorporating gut feelings. Even those which purported to incorporate qualitative and gut feelings from a theoretical perspective seemed to lack practical techniques for incorporating these critical factors into making real world decisions. This deficiency often resulted in decisions that everyone knew were wrong, but it was often difficult to dispute the results of the often complex and highly mathematical methodology that appeared to be championed by the leadership. Questioning these classic approaches was often viewed as a bad career move. Research by Dr. Jerry Harvey illustrates how and why people go along with bad decisions even in the face of tragic costs to their organizations or national priorities. In his video called the Abilene Paradox, this all too human tendency is played out in terrible detail.

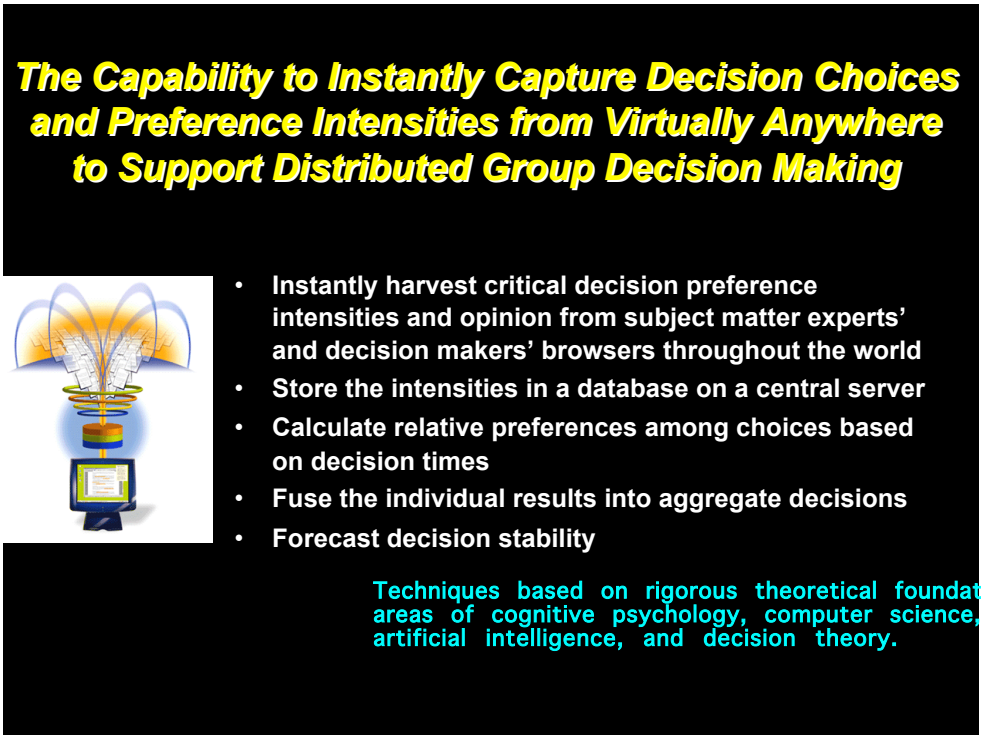
In meetings with military decision makers, we find that they feel the same problems exist in military decision making because of large, complex, distributed, and poorly understood decision methods, not processes, which are known to provide highly questionable results. From the

practitioner's perspective, they feel that military decision making is trapped within a highly confident Newtonian world where recent experience demonstrates that the war fighter's environment is a highly personalized fast paced quantum universe where classic decision making offers only second rate solutions. There is a strong opinion that the service schools and military science establishment have avoided research in innovative decision making and prefer the safer areas of conventional thinking. The facts may be debated; however, the opinions are real.

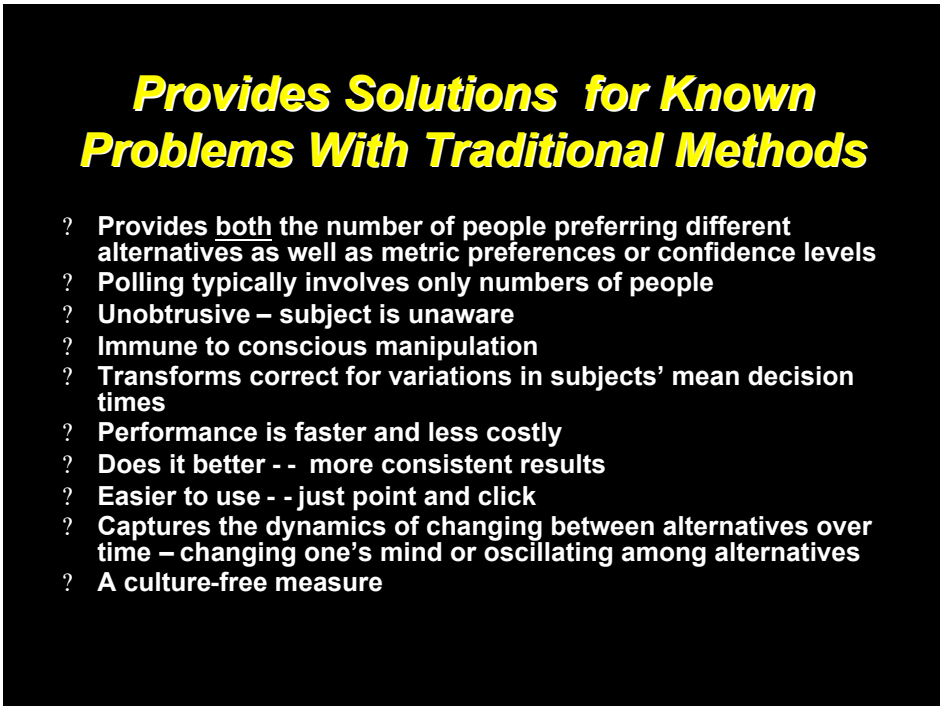
In interviews with military contractors we find similar reasoning. Some feel that, since they have invested years and are highly credentialed in classic methods, if radically different approaches come into vogue, their position and tool sets might be viewed as obsolete. Thus, until recently, there was almost no incentive to embrace alternative methods.

The technique that translates decision times into ratio scaled confidence and preference metrics is one such alternative. The alternative methodology is motivated by several of the foundation technologies and an approach employed in the field of artificial intelligence - specifically artificial neural networks - and describes a set of decision analytic techniques as well as a web-centric medium for deploying the application among distributed decision makers. The approach addresses some of the challenges for capturing, fusing, and analyzing decisions, opinions, confidence, and preferences from subject matter experts as well as the general population. The technique is believed to offer features and advantages not found in other approaches.

A summary of the technique and distributed decision support environment is provided in the following illustration.



The decision time, sometimes called response latency, methodology provides solutions to many of the problems associated with classic methods. A summary of the advantages are listed in the following illustration.

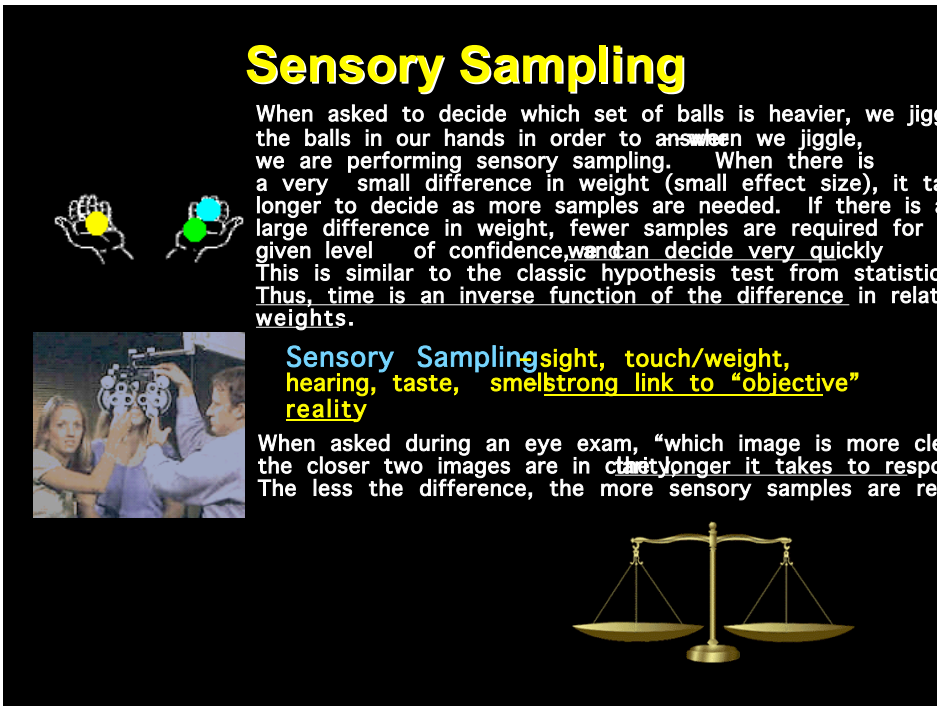


Sensory Sampling is the Foundation of this Approach

We are testing a new kind of collaborative methodology able to capture information from anywhere in the world, from subject matter experts or others, and merge the individual opinions into group decisions. More importantly, we employ subjective and sensory sampling techniques, coupled with the analytic hierarchy process, to translate the time it takes to make a decision between two choices into degrees of preference or confidence.

In sensory sampling, consider, sampling as related to hypothesis testing. For example, if I have two weights that I am holding, one in each hand, and they are almost identical; I jiggle them a bit to determine which weight is heavier. When I do the jiggling, I am actually sampling the weights, this is called sensory sampling, and my judgment as to which weight is heavier is a hypothesis test. If there is a large effect size, meaning one weight is a lot heavier than the other, then the decision is made very quickly, as fewer samples are required. That is highly intuitive so the idea of sensory sampling has high face validity. However, what is also intuitive is if the effect size is small, or the weights are almost the same, it will take a much longer time to make the decision as to which weight is heavier; that is, more time equates to more samples. Sensory sampling has a strong link to objective reality in terms of variables such as weight, brightness, temperature, and related phenomena.

The general idea of sensory sampling is summarized in the following illustration.



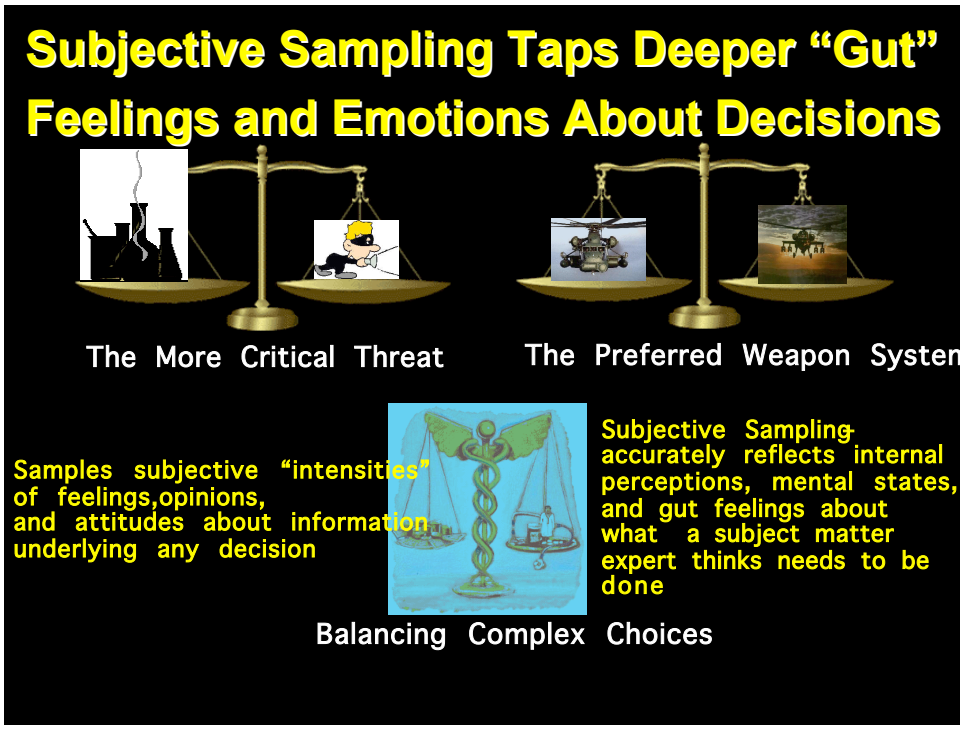
As a thought experiment, imagine what happens during an eye examination when one is being fitted for a lens prescription. As the doctor asks which image is clearer, at the beginning, when one image is a lot fuzzier than the other, the responses come quickly; as the image quality becomes more similar, it takes a longer time to make a decision. That is because as the images become more similar, more samples are required in order to make a decision at a fixed level of confidence - - a classic hypothesis test. That is, degrees of confidence or preference are inversely related to the decision time. This paper reports on that relationship, its application in software, and integration within a web-centric decision support environment.

SUBJECTIVE SAMPLING

As mentioned, sensory sampling deals with objective reality – brightness, weight, and related phenomena. However, we are more interested in what is called call subjective sampling; that is what occurs when subject matter experts assess threat levels, risk, the better weapon system, or the utility of different courses of action. In these cases, a similar process is occurring where experts sample the differences in qualitative or affective phenomena.

Consider the problem where subject matter experts must assess the efficacy of different units conducting test and evaluations exercises. It is very difficult to assess unit performance on a 1-10 scale. We know this because that is what the subject matter experts report. However, they also report that making a pairwise decision among the units with respect to which unit demonstrates the better performance is a relatively easy task.

The concept of subjective sampling is summarized in the following illustration.



What we have done is to develop a method that will capture the subject matter experts' decisions and translate their decision times into confidence and preference metrics; then fuse the metrics into a group assessment. We have found that this technique is far superior to classic methods, is quicker to apply, is better accepted by subject matter experts, and provides better results.

In working with subject matter experts, military officers, high level civil servants, and corporate executives, we uniformly get the same reports. When forced to use a 1-10 scale or sliding bars to assess decision confidence, these people had no problem in expressing their opinion very strongly on the topic with comments such as; "you know we don't think that way… we don't think that way at all… it just does not make sense for what we do"

However, if we offer choices in a browser window, and ask experts or executives to just click on the preferred choice; that can be done very quickly and with no complaints; then, the choice selected and time is captured and stored. From that information, complete and highly accurate confidence and preference intensity metrics are calculated. More importantly, when we ask those same individuals if the relative values, presented graphically, actually represent their true feelings, the answer is always "yes". Thus, there is an extremely high face validity in the process where people quickly understand how the process works, are comfortable with the concept, and agree with the results.

Fusing Individual Results into Group Metrics

To better illustrate the concept, an example is provided where we employ a number of subject matter experts to assess relative threat intensities. The example is summarized in the following illustration.

Applying This Method To A Real Scenario

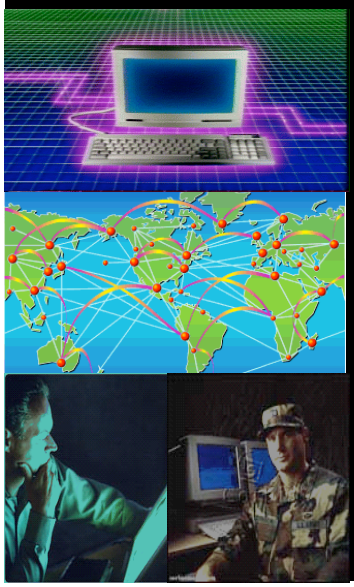
Subject Matter Experts (SMEs) assess the relative risk of Threat 1, Threat 2, Threat 3, Threat 4, and Threat 5.

Our goal is to assess relative threat risks as well as decision stability for the group of SMEs.

For purposes of simplicity, the first part of the analysis will consider only Threats 1 3.

The subject matter experts will be asked to assess which threat is the most severe using the approach summarized in the following illustration.

Assessing the Subjective Risk Intensities for Five Different Threats Via Web -Centric Collaborative Decision Support Environment

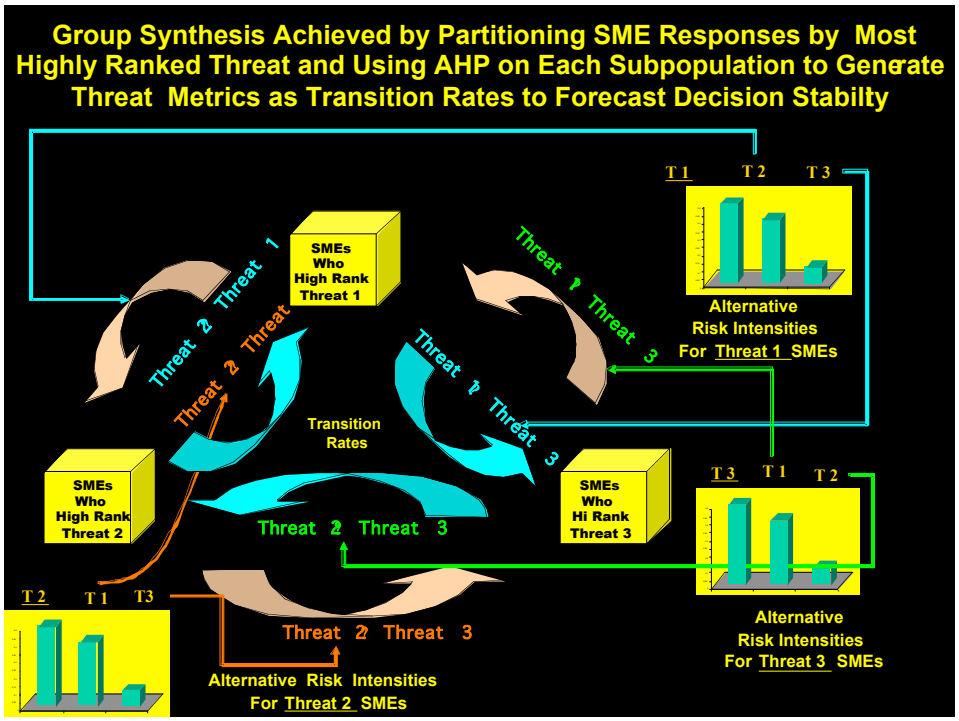


- Subject is Presented With Choice Combinations, Two at a Time, Via the Browser
- Subject Clicks on Preferred Choice Within Browser Window
- The Choice Selected and Time Are Sent Back to the Server
- Responses Clustered by Most Highly Ranked Alternative
- Inverse of Time Function and AHP Used to Calculate Relative Intensities Among Alternatives and a Consistency Measure
- Transition Rates for Decision Stability Metrics
- Generate Decision Metrics

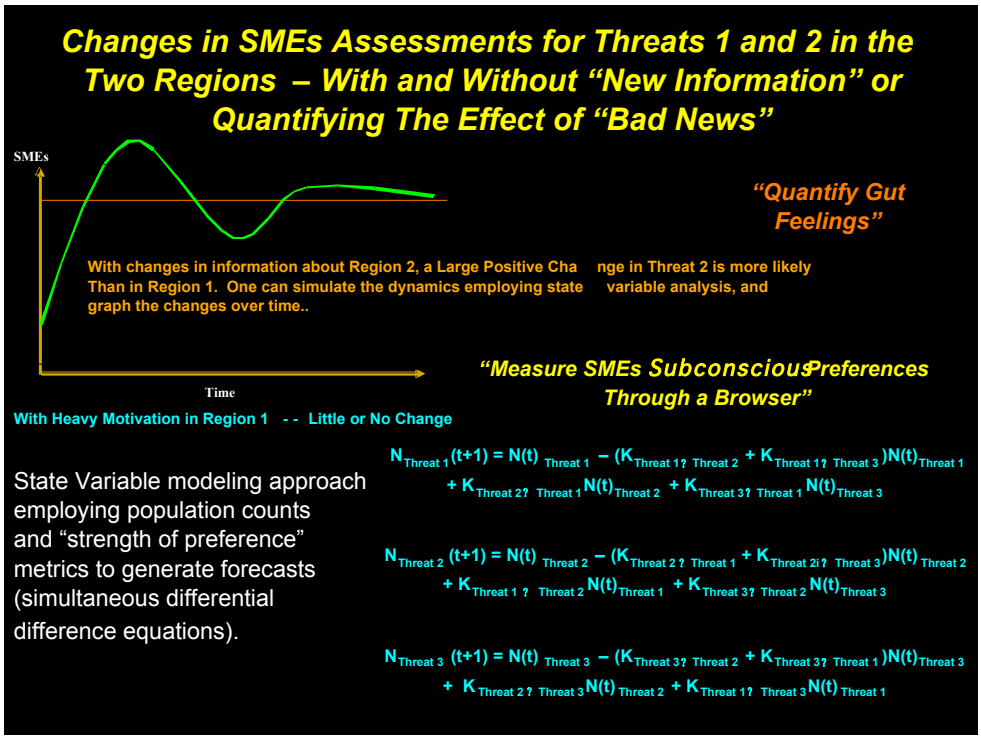
After the subject matter experts assess the five risks; normalized preference intensities are calculated for each expert's assessment. Then, the question becomes how to fuse the different

individual opinions into a single group metric and assess its stability, or the propensity of the decision to remain as it is and not change or oscillate among other decisions. That is, the propensity of the group not to change its mind.

The technique used is to partition the individual assessments by their top choice, then calculate the fused group metric for each top choice using a geometric mean. This results in a set of normalized metrics for each choice as well as the number of experts who picked that choice as top. This can be represented as a state variable model where the metrics are the Markovian transition rates between the states. This model is summarized, for three choices, in the following illustration.



The graphic model can be represented mathematically as a set of linked differential difference equations illustrating the time dependency of experts changing their mind. That situation, the changing one's mind, is represented by an expert moving from one state to another. Interestingly, this model captures and represents the concept of changing one's mind and how that affects decision stability. The mathematics for the three states is summarized in the following illustration.

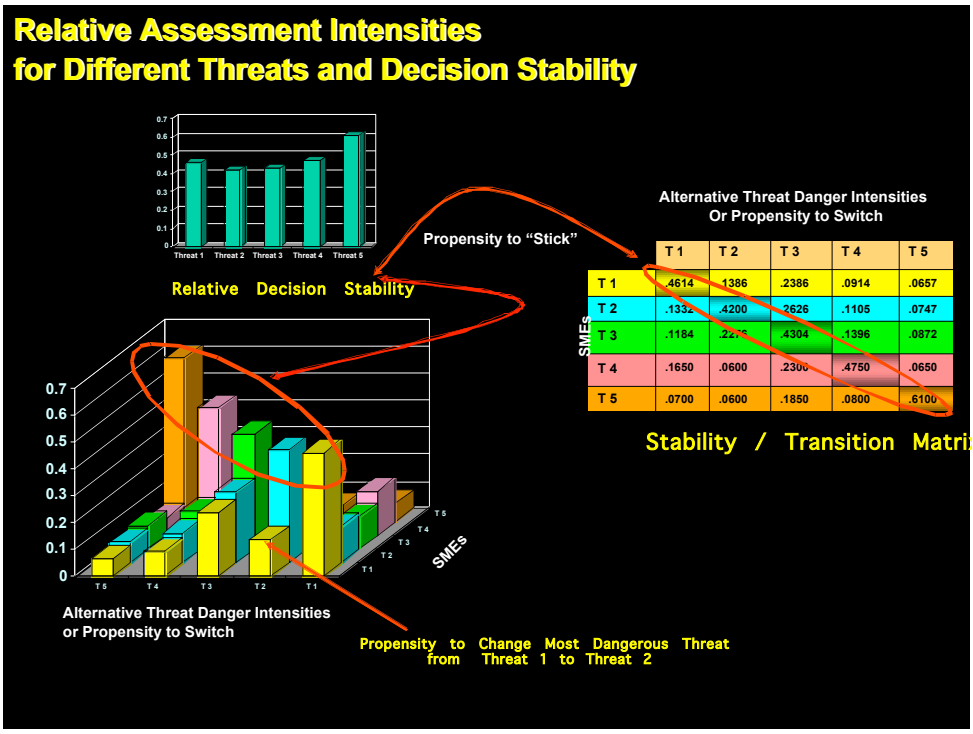


In the next illustration, we summarize three different ways of examining the output of the analysis. First, in the lower left portion of the illustration, note that the vertical axis represents the relative preference intensities of the different threats. The horizontal rows represent a particular choice state or cluster where all SME's associated with that state selected the associated threat as the most severe. Thus, the state associated with Threat 1 is colored yellow. The first element in the row, to the far right, is the geometric mean of the relative preferences of all SMEs in that state for the choice, Threat 1, which is associated with that state. Since SME's in that state were selected as choosing Threat 1 to be the most severe, it stands to reason that that element, on the far right, is the largest. The other elements of that row represent the GMs of the second, third, fourth, and fifth choices for the SMEs associated with that state; that is, their propensity to switch to an alternative choice (state). In the Threat 1 state (yellow row), the propensity to switch to Threat 2 as the most severe is the magnitude of the second element, to switch to Threat 3 is the third element, and so on. Then, the second row back, the blue row, represents the Threat 2 state; in that row, the first element to the far right, represents the alternative preference or propensity for an SME in that state (preferring Threat 2 as most severe) to switch to state 1 (Threat 1 as most severe), the second element is the SMEs preference for Threat 2, and so on. Note that since SMEs who chose Threat 2 as the most severe were all placed in that state, it stands to reason that the GM for Threat 2 would be the highest for that state. In essence, that is the case for all states.

The summary in the upper right side of the illustration is a view of the three dimensional bar chart from above, looking down; and containing the actual magnitudes of each bar.

Note also, that if we traverse the diagonal, we see that those elements are always the greatest within their respective row. The collection of the diagonal elements is summarized in the upper left portion of the illustration and represents the relative stability of the choices in terms of the

propensity of the group to either settle on one or more choices or oscillate among different several choices.



SUMMARY

We have presented the general idea for a method of calculating relative ratio scale preference and confidence metrics employing the time it takes to make a decision in a paired-choice scenario. We employ a modified Analytical Hierarchy Process (AHP) approach to scale the times; however, that was a proof of concept choice. It would have been just as easy to use multidimensional scaling or any one of a number of different scaling techniques. We understand that there is some controversy with the AHP approach; however, there is some controversy with every other approach. Thus, it is important to understand that the substance of the technique is based on a computational model of the brain function, sampling theory, and the general notion that the smaller the effect size, the more samples are needed to reject an hypothesis at a fixed confidence level. The scaling method is merely a convenient way of operating on a non-linear time function to create relative magnitudes and a measure of consistency among the calculated magnitudes.

We also report on a method for fusing or synthesizing the results of an individual into a group metric. Here we examine the individual responses and segregate by the top choice. Thus those identifying Threat 1 are lumped together as well as those identifying Threat 2, and so on. The logic here is similar to a market research analysis where the choices might be relative preferences for Coke, Pepsi, or Sprite. Those preferring Coke would be lumped into the Coke State and the same for Pepsi and Sprite. Coke would view the Coke state as representing their customers, with Pepsi and Sprite doing the same for their states and customers. Then we

calculate the geometric mean of the preferences of those within each state to obtain a group metric for preferring that state as well as alternative preferences for other states or products.

FREQUENTLY ASKED QUESTIONS

Some people take longer than others when responding to questions. How does this affect the results?

The resulting metric is normalized and assesses the ratios of the decision times, so typically slow or fast people do not present a problem with the technique.

The decision makers, employing browsers and the Internet, are connected to the central database via telecommunications lines. If one had a bad connection, if the Internet suffers severe congestion, or variations in transmission time occur, might that cause noise in the results?

Not at all, the decision time and other data are captured on the client side, in the browser, and sent back to the server as data. Transmission times are not a factor.

What if someone does not care, randomly enters data, or has no opinion; might that cause a problem?

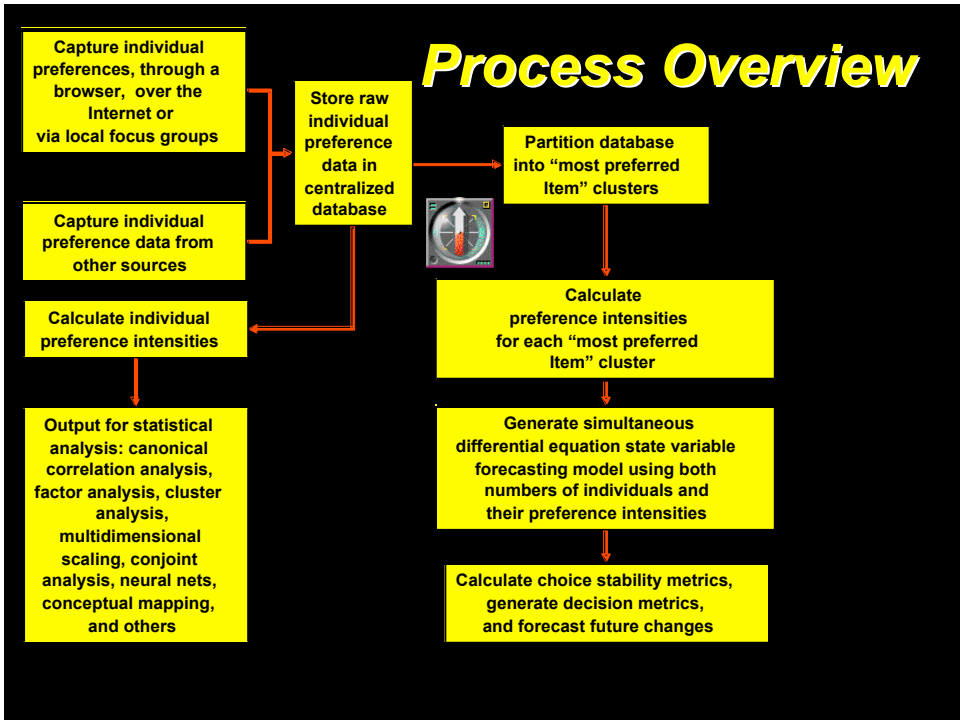
That can cause a problem even if we are not using this technique; however, in our case, we calculate the consistency in a subject's response and store that number along with the response data. Consistency is a mathematical relationship involving the transitive property of an individual's responses. It is a complex relationship among the responses, hard to fake, and very unlikely to occur by chance. Thus, random entries, or entries by someone who neither knows anything about the topic nor cares would generate very low consistency metrics. Since we collect, for each respondent, a consistency metric, it would be easy to identify those who were not taking the exercise seriously.

Do subject matter experts respond differently than non-experts?

As one would expect; subject matter experts exhibit a much higher consistency in their results than do non-experts.

PROCESS OVERVIEW

A general overview of the approach and flow diagram of the process is summarized in the next illustration.



GENERAL REFERENCES

Banagi, M.R., and Greenwald, A. G. [1994]. Implicit sterotyping and prejudice. In M. Zanna & J.

Cartwright, D. [1941] Decision-time in relation to differentiation of the phenomenal field. Psychological Review, 48, 425-422.

Clemen, R. T. [1996] Making Hard Decisions; Duxbury Press, 265-298

Crosby, F., Bromley, S., & Saxe, L. [1980]. Recent unobtrusive studies of black and white discrimination and prejudice: a literature review. Psychological Bulletin, 87, 546-563.

Dashiell, J. F. [1937]. Affective value-distances as a determinant of esthetic judgment-times. American Journal of Psychology, 50, 57-67

Dovidio, J.F., and Fazio, R. H. [1992]. New technologies for the direct and indirect assessment of
attitudes. In J. Tanur [Ed.], Questions about Questions: Inquiries into Cognitive Bases of Surveys 204-237. New York: Russell Sage Foundation.

Fazio, R. H. [1995]. Attitudes as object-evaluation associations: determinants, consequences, and correlates of attitude accessibility. 247-281. In R. E. Petty & J. A. Krosnick [Eds.], Attitude

Strength: Antecedents and Consequences. Hillsdale, NJ: Erlbaum.
_____. Jackson, J. R., Dunton, B. C., and Williams, C. J. [1995]. Variability in automatic activation as an unobtrusive measure of racial attitudes: a bona fide pipeline? Journal of Personality & Social Psychology, 69, 6, 1013-1027.
_____. and Williams, C. [1986]. Attitude accessibility as a moderator of the attitudeperception
and attitude-behavior relations: an investigation of the 1984 presidential election.
Journal of Personality and Social Psychology, 51, 3, 505-514.

Festinger, L. [1943] Studies in decision. Journal of Experimental Psychology, Vol. 32, No. 4, 411-
423.

Forman, E. [1999] Personal communications with Professor Ernest Forman, The George Washington University, School of Business and Public Management, Washington, DC.

Gaertner, S. L., and Dovidio, J. F. [1986]. The aversive form of racism. In J. F. Dovidio & S. L. Gaertner [Eds.], Prejudice, Discrimination, and Racism 61-89. Orlando, FL: Academic Press.

Harmon, P. and King, D. [1985] Expert Systems - Artificial Intelligence in Business; John Wiley &
Sons, Inc. 41-43.

Kahneman, D., Slovic, P., and Tversky, A. [1999] Judgement under uncertainty: Heuristics and biases; Cambridge University Press

LaBarbera, P. A., & MacLachlan, J. M. [1979]. Response latency in telephone interviews. Journal
of Advertising Research, 19, 49-56.

Lam, A. [1998] Tacit knowledge, organisational learning and innovation: a societal perspective. DRUID Working Paper No. 98-22, Danish Research Unit For Industrial Dynamics

Marshall, K. T. and Oliver, M. R. [1995] Decision Making and Forecasting, McGraw-Hill, Inc. 240-
241.

Medsker, L. [1998]. Personal communications with Professor Larry Medsker, American University, Department of Computer Science and Information Systems.

Nisbett, R. E., and Wilson, T. D. [1977]. Telling more than we know: verbal reports on mental processes. Psychological Review, 84, 231-259.

Polanyi, M. [1962] Personal knowledge: towards a post-critical philosophy. New York: Harper Torchbooks.

[1966] The tacit dimension. New York: Anchor Day Books.
Saaty, T.L. [1977]. A scaling method for priorities in hierarchical structure. Journal of Mathematical Psychology 15 79-84

[1994] Fundamentals Of Decision Making And Priority Theory with the Analytic Hierarchy Process, Volume IV, 1994, RWS Publications, Pittsburgh, PA., 8-127.

_____[1995] Decision Making for Leaders - The Analytic Hierarchy Process for Decisions in a Complex World. Third Edition. RWS Publications, Pittsburgh, PA., 70-92

[1999] Personal communications with Professor Thomas L. Saaty, the University of Pittsburgh.

Sigal, H., and Page, R. [1971]. Current stereotypes: a little fading, a little faking. Journal of Personality and Social Psychology, 19, 247-255.

Tyebjee, T. T., [1979]. Response latency: a new measure for scaling brand preference. Journal of Marketing Research, 16, 1, 96-101.

Demonstration of a Typical Ontology-Based Collaborative Agents System: SEAWAY

Col. Tony Wood (USMC Ret.) and **Dr. Jens Pohl**
Collaborative Agent Design Research Center
Cal Poly, San Luis Obispo, California

SEAWAY: Advanced Decision Support to Expeditionary Operations

Do you know what a parable is? When you're over 50 you don't tell jokes. You tell parables. Bear with me a moment for a parable.

The shadows were lengthening in the swamp and the bunny rabbit came hopping down the trail and the blind snake came hopping down the trail. And the blind bunny rabbit smacked into the blind snake and they recoiled, and the blind bunny said, "Who and what are you?" and the snake said, "I don't know. Who and what are you?" And so they decided to find out. And slowly that snake wrapped himself around that bunny rabbit and he said, "You've got large ears to hear with and a bunny rabbit tail and rabbit whiskers and big hoppers. I think you're a bunny rabbit." And the blind bunny rabbit said, "Oh what joy! This is the greatest day of my life! I know what I am! Now, let's find out what you are." And very slowly that snake uncoiled and lay down on the dust of the trail and the bunny hopped over and reached out: "Cold skin, small beady eyes, speak with a forked tongue, no visible sex organs…I think you're a lawyer!"

In the ten years that I have been working on decision making you're never quite certain what the outcome of what you start is going to be. And the law of unintended consequences is very much alive and well, particularly in developing new applications for decision support. Today I am going to provide a quick overview of the SEAWAY decision support system.

In San Luis Obispo we have seventy-seven SEAWAY systems which are being prepared for fielding, and we are deep into the design of the follow on version. So, we are discussing a decision support system which is operational. Before we explore SEAWAY, we probably ought to talk about defining decision making problems and applying decision support.

In the case where the senior decision maker has poor decision skills, even the best decision support will make only the most marginal of difference. However, good decision support can make a huge difference if you have just an adequate decision process and adequate decision-making skills at the top. But without adequate decision-making skills supported

by an adequate decision process, all the decision support in the world won't make much difference.

My second observation on the design of decision support systems is that we have to be careful not ask the computer to do something which it doesn't do well. Not because it's unfair to the computer, that's nonsense – but because it will undercut our own mission and deceive us.

Computers don't conceptualize. Point one. They don't have intuition. Point two. And, three, they do not do well in analyzing subtlety on the modern battlefield in terms…especially in terms of urban operations and political considerations. With this in mind, we need to be careful when we talk about decision makers not forget to use this very elaborate massively parallel processor we've got up here on the top of our neck to assess the subtlety of the battlefield and the campaign.

Now, when conducting seminars at the Naval Post Graduate School in Monterey, I compare the battlefield that existed prior to Afghanistan with the battlefield that exists today. Consider just a few of the contrasts with which we are now faced – but which are not reflected in our decision support tools most of which were developed in the Cold War period. The gross battlefield of the north German plain, large forces, no ROE, very, very large movements, few or no rules. A battlefield where precision was not critically important, and one that rewarded mass, depth, and size. The characteristics of this cold war framework defined United States military decision support initiatives and, to a very large extent, continue to do so today. However, we have a problem; this defining battlefield has disappeared to be replaced by one which is quite different.

Although the "E" word is not fashionable, we are closer to dealing with a situation as a military which is more akin to the British situation between 1814 and 1914 than we are to any other period I can think of. So if that's the case, if we're dealing with subtle battlefields with political and military mixtures in places like Afghanistan and Iraq and elsewhere, then we also need to remember that the individual decision-making skills from private to general are probably as important as decision support and deserve at least as much attention.

Second point: Military decision support systems are designed for experienced professionals – not amateurs. Decision support systems are not designed to raise the incompetent and inexperienced to an adequate level. The systems are designed to be leveraged by experienced professionals who understand both the limitations and the strengths which the computer offers. The poorly trained and the inexperienced will substitute slavish dependence for calculated evaluation of results.

Third point: There's a moral dimension to the relationship between a decision support tool and the decision maker. Depending on where you come from, you will agree or violently disagree with my next couple of comments. However, in my view, we must never place the computer between the decision maker and the responsibility to make a decision –

especially one involving a decision on life and death. Never. When we do that what have we done? There is no longer a linkage between the person and the action he or she has directed. There's no linkage between the decision to take violent action and the consequences. If the computer is between me and that decision, then all I did was exercise the computer. At any rate, I think what I have expressed is largely a Marine Corp point of view, but it's one that I believe is well worth thinking about.

For the last three years I've been working with about thirty Navy and Marine officers designing and building SEAWAY, a decision support tool for the MAGTF, the Joint Task Force, and for expeditionary warfare in general.
SEAWAY's design combines human strengths with computer strengths in a collaborative framework. On the human side the system design assumes that conceptualization will come from the user. It is in the design of the system architecturally. Secondly, the design assumes that the generation of a conceptual scheme of maneuver and its description will come from a human because this sort of conceptualization is a uniquely human skill. The design assumes that the computer will provide the ability to track hundreds of thousands of items. It assumes that the computer will stand back-to -back watches without getting tired, and that the computer will rapidly convert our conceptual schemes of what the force is going to do into the logistics and the delivery of "how" it's going to do it. So, architecturally, the design "leads to strength." When you build a decision support tool "you must "lead to strength" and combine the human strengths with those from the computer. Don't ask the computer to do what it can't do (such as conceptualize) any more than ask us to track thousands of items individually.

SEAWAY provides tools to support the Joint Task Force and MAGTF at the operational level of war. Why the Joint Task Force and why the operational level? Because we have turned "TPFDDing" into a cottage industry. Because we have spent the last 15 years building strategic tools which we've rarely used. Because we have focused on the strategic level of war rather than the operational because it is easier to deal with. Because we have done very little to help the force where war is actually waged -- at the operational level. Because there are no tools for the Joint Task Force commander. Because he has no capability to analyze theater logistic posture and compare it to the support needed for his intended campaign. Because he has no capability to translate his intentions into what it may take to support them. None of the tools needed to support these functions exist. And, even as we discuss the absence of these needed tools we are standing up permanent joint task force headquarters. Amazing, isn't it? Well, that's why we built SEAWAY.

With these thoughts in mind, I went to ONR about three years ago with a vision and said, "Look, we're talking about supporting widely dispersed operations at deep inland locations whether the focus is Army deep maneuver or Marine operational maneuver form the sea, or similar joint concepts. We're proposing inserting forces and supporting them at great distances inland in joint and coalition operations. That means that the forces will be supported at the end of a helicopter-borne umbilical. That means that as fast change occurs (and the only certainty on the battlefield is continual change) we're going to be forced to recalculate the support requirement. Think about Iraq. Think about the first Marine

division's march to Baghdad. Think about how often unanticipated even by the wildest of planners that constantly changing operational requirement had to be altered.

As I said, the only certainty on a battlefield is change. You can be certain everything's going to change and that the plan is going to be great until the first shot is fired and not a second farther. After that it's a new plan. So, the underlying assumption in we built into SEAWAY is that everything will change all the time. This new decision support tool would be built to provide recommendations in the face of continuous change.

So, we can establish several characteristics, which SEAWAY had to have. First, lead to strengths, human and computer. Second, provide assistance in a familiar fashion (Don't give staffs a tool that has a whole new face on it). Third, provide *flexible* tools. Why? Because we don't know what the force is going be faced with. We don't know the kind of campaigns. Nobody would have predicted Afghanistan or Iraq in 1998. They might have predicted other things, but those two wouldn't have been at the top of the list. So tools which can *adapt to any situation*… because we can't predict what the operating forces will face. Fourth, compliment the established planning process. Provide tools which compliment what our forces already understand and exercise. Fifth, make the tools collaborative. In December 2001 five staffs employed SEAWAY at separate locations simultaneously for three days. All at the same system at the same time from four or five different locations. Sixth, make it fast and accurate. Identifying change isn't the battlefield objective – the objective is *spotting its implications and exploiting it before the other guy can.* Finally, seventh, make it *useful*. Not only do the JTF's not have any tools, but many of the tools we've given them are either so difficult to use or so trivial that they don't use them. Decision support should deal with very difficult issues in complex decision situations in a fashion familiar to the user.

Constant change. I mentioned that the underlying assumption in SEAWAY's design was dealing with continuous battlefield and theater change. What sort of change? The *resources* available to the Joint Force Commander change continuously as consumption and re-supply exercise their opposite effects. The *battlefield itself continuously changes*, whether it's a battlefield like Iraq, or whether it's something far less well-defined such as Afghanistan, or a combination of both. The friendly, enemy, and neutral elements are all dynamic. As a result of these factors and others, *plans must change* all the time. As a result, the JTF commander is faced with three continuously changing cycles all of which interact. SEAWAY is designed to deal with these continuously changing cycles, to accept constant changes, and to provide alerts, warnings, recommendations, and plans – and to change these as change demands.

What tools does a JFC have to deal with change? Damn few. While I was a Chief of Staff in the Pacific, we formed five real JTFs -- and each time it was a pick-up ballgame. Each time we contributed the tools we thought could help but they were pretty poor. So, SEAWAY was and is a product of frustration as well as a product of commitment and need. It must support single service, joint, and coalition operations equally and easily. As

I think you'll see during the demonstration, it can do so. And it should do so rapidly —whether generating options or assessing their supportability.

The tools in SEAWAY were also designed to assist professionals in identifying opportunity costs and assessing risks. The important word there is "help" – not do it for them. I'm probably telling some in this audience how to suck eggs, but I find that there's a widespread misunderstanding as to the difference between "opportunity cost" and "risk". It really is important to understand the distinction. *Opportunity cost* is an action foregone as a result of your decision to execute a particular course of action. In other words, it's something you can no longer do. It is the *cost of selecting that course of action*. For instance, if I decide I'm going to shoot up 85% of all of my artillery ammunition tonight, then tomorrow morning one of the opportunity costs of that decision is an inability to provide artillery fires until I can get re-supplied. That's an opportunity cost.

It's not a risk. Risk is the likelihood that something will happen times the consequences if it does happen. Using the artillery y example, if we are engaged in a United Nations support operation, firing up all the artillery rounds may have very little consequence, and hence the risk is slight. However, if we were engaged in North Korea, it would be an entirely different and far more serious risk situation. So, a good decision support tool at the Joint Task Force level should help us identify opportunity costs and certainly should assist in assessing the associated risk. Philosophically, I would never build a system that assesses risk. I would build one that provides indices and allows professionals to assume that responsibility. I continue to believe that the responsibility for risk assessment must remain squarely on the shoulders of the commander and his staff.

The graphic below presents the basic logic flow of Seaway. Many of you are thinking, " I've seen that before." and you bet you have. It's the logic of the military planning process. First, A commander generates a notion. Then, using IPB and LPB tools in SEAWAY we can quickly generate a scheme of maneuver on an interactive battlefield. *Interactive*? What does that mean? It means that as I draw the rivers in, the agents understand that they are rivers. If I try to draw a scheme of maneuver across that river for a tank unit they will alert. They will look at that unit and tell me "Sorry, tanks don't swim. You need to find a bridge or go somewhere else." In other words, they understand what's on that map. They understand what's in the unit. They understand the terrain and the weather. If we create a swamp and we try to go through it, they're going to adjust the rate of advance and all kinds of other things in the logistics.

So, returning to the logic flow, we generate a scheme of maneuver. First we task organize the force to be employed. SEAWAY can employ units as task forces, as individual units, or as combinations of task forces and units. It is adaptive because we have to be adaptive as we fight. It is doctrinally neutral, allowing the user to employ the force according to any doctrine that is appropriate. Just as we can create allied and friendly task forces, SEAWAY supports creating enemy task forces and then employing these. Although this capability has not been tested, everything that we're going to discuss today concerning

friendly forces can be accomplished with enemy forces, neutral forces, and allied forces. You can task organize all four, you can employ all four, and you can assess supportability, opportunity costs, and risks for all. Now, at this point I don't know where this capability is going to lead because we really haven't been able to test it yet. However, there's some real excitement about it building in the intelligence community about it.

Once we have generated a scheme of maneuver on SEAWAY's interactive battlefield, we can pose key questions aimed at assessing supportability, opportunity costs, and risk. Question one: is it supportable in terms of *inventory*? Question two: can I *deliver* it to with the transport assets I have? And, question three? *At what price* (in both cases)? The question of price focuses on opportunity costs and risks. For example, the "price" of delivery can be measured in lost operational flexibility for the joint task force. Because we're operating at a deep inland location, all logistics must be delivered by helicopter. However, maneuver also depends on helicopters – the same helicopters. That's the built in tension in emerging doctrine, especially that supporting sea basing. A tool such as SEAWAY must assist in rapidly furnishing decision support to commanders and staffs in answering the question of *"At what price?"*

A good operational planning team at I MEF can generate a scheme of maneuver in SEAWAY in about 10 or 15 minutes for a MEB of 12-15,000 troops. Once that scheme is complete, the OPT will give SEAWAY guidance on expected intensity, phases in the scheme, and other key guidance. SEAWAY will then rapidly perform several functions. First, agents will translate the *operational* scheme of maneuver into a *logistic statement of requirements* in about ten minutes. That statement is a recommendation of *what must be delivered in what quantity to what landing zones for which units in what time frame in order to support the phased scheme of maneuver* generated by the OPT.

Next, we arrive at our first major decision point. Do we have the fuel, water, food, and ammunition inventory to do it? Because SEAWAY is fully interoperable with ICODES (and hopefully with TCAIMSII when that system is proved), agents can compare what is required to execute the scheme of maneuver phase-by-phase with what is currently available and what is en route to the theater. The result is to identify the deficits, where stocks are located that could offset them, and when new stocks of the short items are die to arrive. So, as a Joint Task Force commander, at any point in time, I can see what is coming and what is here, and how well it supports my proposed course of action. Now, with agents translating operational courses of action directly into logistic requirements and comparing these with available supplies, we have given the JFC a valuable tool with which to shape the theater out perhaps thirty days.

In this process we would probably receive alerts with messages such as the fact that we don't have enough 155 to execute at the intensities we have specified. Well maybe we do and maybe we don't. You and I may know very well that we do, and that the deficit is in fact very minor. However, the agents are making recommendations based on a set of rules. Recommendations – not decisions.

Let me talk for a moment about decision support systems and the importance of *transparency*. My advice is simple: *If you can't open the hood and look at the basis for every computation and how the agents are functioning, don't buy it and don't use it.* It's that simple. I think the rule is ironclad. Don't buy it and don't use it if you can't open it up and can't look at it. Every computational basis in Seaway is transparent to the user. That's the good news. The bad news is you'd better protect access to these important files.

Once the commander has determined that the scheme of maneuver is supportable in terms of inventory, the question becomes "Can I get it there, and at what price in terms of operational flexibility?" First, we identify the assets which are available to deliver supplies and equipment. There are tools which support reserving helicopters and other delivery craft down for maintenance, to be used in assaults and other tactical operations, and various other categories used by the operating forces. SEAWAY will then load every remaining helicopter (and LCAC if these can be employed) *individually* by tail number, using the performance characteristics for that particular craft. The agents in SEAWAY will then create a detailed sortie-level phased delivery plan that exactly corresponds to the demands and the timing of the parent scheme of maneuver.

Why go to such lengths? Because SEAWAY was designed for war fighting assessment and this sort of accuracy and realism is way beyond "tonnage divided by numbers of aircraft". If I have 12 helicopters on the deck of a LHA how many of them do you think will have the same characteristics? Perhaps three? The other nine will have all different lift characteristics, and these might vary by as much as 40%. It gets better than that. What's the difference between a helicopter lifting off and LHD seaward of Wonsan in February and lifting off and LHD seaward of Wonsan in July? It may be as much as a 40% variation in payload. Heat and humidity take their toll on helicopters. So, to summarize this step, Seaway allows you to characterize and to set performance characteristics for every helicopter individually as you build the delivery plan. Agents then load each bird individually and build a sortie level plan involving multiple ships, multiple tactical bases ashore, and multiple forward landing zones. It is complex, and it ought to be for that is the nature of warfighting.

SEAWAY may take as long as twenty or twenty five minutes to generate all of the sorties and decision aids describing a delivery plan of 100 sorties or more.. We may also receive agent alerts indicating that the supplies and equipment needed for the scheme of maneuver can't be delivered in the time element which we have prescribed. In this case the agents offer us several different options designed to bring the plan into an acceptable state. We can move the sea base; we can level supplies between landing zones; we can increase transportation assets; and, if we still can't deliver the needed supplies in the timeframe required, then the course of action is unsupportable in terms of delivery. But, for the first time, because SEAWAY is distributed and collaborative, we all know it's not supportable, whether the JFC at sea, the GCE commander ashore, or the J3 over there on the top of a mountain. And, we can all see why it's unsupportable without staff meetings and endless briefings. We can all see the same explanatory screen at the same time.

What does this do to *tempo*? It can dramatically speed it up. What does it do to *adaptation* if I can now do three or four schemes of maneuver in a morning that previously took three days? What does it do to *accuracy* if we've got agents tracking hundreds of thousands of items and rapidly calculating the support for each phase in a scheme of maneuver? N75 used Seaway two weeks ago in an analysis of future LHA-R requirements. Some of the MEB delivery plans were 180 sorties long and involved several hundred thousand items for delivery.

Now. Let me pause for a minute and address how SEAWAY creates and then employs ships to build a sea base. Because ICODES is fully interoperable, agents in SEAWAY can digitally create any US ship including all service pre-positioning vessels, all L-class ships, and all black bottoms owned or leased by TRANSCOM. Additionally, for the almost 300 ships in the current system inventory, SEAWAY knows the deck cyclic rates. It knows the helicopter spots. It knows the L-CAC wells, and it knows many other characteristics, all of which may be adjusted by the user. You can increase the helicopter spots. You can increase the wet wells if you want to do all that. But the defaults are the clear values of the ships as these exist today.

SEAWAY is not designed as a current battle management tool. We're building a planning and assessment tool. So don't mix up battle management or war-gaming a current battle situation with planning and assessment. Battle management is "right now", and is essentially reactive. SEAWAY is really a set of tools designed to support the staff in performing future operations and future plans – operations to be conducted two to 30 days out. It's tools could also be used to validate and assess the extent to which an existing theater war plan could actually support a prescribed force under a specified set of operational conditions using the logistics which have been planned. There are undoubtedly many many more uses,

A question always arises on how the agents calculate the logistics for each phase in a proposed scheme of maneuver. What do the agents know as that is occurring? They know the distances and the forms of maneuver which have been prescribed (some are more consumptive than others). They know every vehicle in a unit or task force and what it consumes. They know every vehicle in a unit or task force that shoots, and what it shoots at each specified intensity. And because we gave it guidance on the scheme of maneuver, they know the expected intensities. The agents are observing and calculating constantly as we task organize, select objectives and forms of maneuver, receive weather conditions and their impacts, and provide commander's guidance. Logistics is now part of the course of action generation process rather than an inaccurate and much delayed postscript.

There are many capabilities that have been asked for in the next SEAWAY, Version 3.0. It will include the capability to generate all supporting plans for the STOM assault and a great many other things, including support not just to rotary wing aviation but also to fixed wing aviation. Other things that have been asked for that are well within the scope of this kind of technology is clicking on a river to get its flow and its width, or getting a building's

composition or many other significant intelligence –related advances. All of that can be added.

In summary, as an example of advanced adaptive decision support, SEAWAY is "different strokes for different folks". Adaptive decision support systems should be useful tools. For the acquisition community, Seaway is being used to model future ship capabilities. The Marine Corps is looking at it from the standpoint of how to support operational maneuver from a sea base, and what kinds of formations are supportable under what kinds of condition, doing what sort of combat. The operational planning teams have used it on the West Coast to generate schemes of maneuver and to quickly assess their supportability. The combat developers at are exploring the new concepts by building schemes of maneuver under different kinds of weather and different kinds of terrain to see what they result in, and introducing new equipment, new trucks. Or, for example, a 22% reduction in fuel consumption – what does that do to free helicopters from logistics delivery missions for assault support? The impact could be enormous; a less consumptive force could have a significant impact on the helicopter requirements to support it. SEAWAY can help us get these answers and many, many more.

I thank you for your attention. Thank you very much.

Countering Threats to America's Public Telephone Networks

Dr. Sujeet Shenoi, University of Tulsa, Tulsa, Oklahoma

Due to the sensitive nature of the material covered by Dr. Sujeet Shenoi, we are unable to include his presentation in these proceedings.

Internet-Telephone Network Convergence: Themes and Security Issues

Dr. Anthony Meehan, University of Tulsa,
Tulsa, Oklahoma

Due to the sensitive nature of the material covered by Dr. Anthony Meehan, we are unable to include his presentation in these proceedings.

Multi-Agent Modeling of the Urban Operational Environment

Frederick J. Diedrich
Aptima®, Inc.
12 Gill St., Suite 1400
Woburn, MA 01801

Paper Presented at the Office of Naval Research Workshop on
Collaborative Decision-Support Systems
September 10, 2003
USMC Base, Quantico

October 30, 2003

Portions of this presentation were based on work that was performed in conjunction with a Small Business Innovative Research Contract, number DAAD17-03-C-0013, with the U.S. Army Research Laboratory, under the direction of Dr. Thomas Cook. The author would like to acknowledge the contributions of Kari Chopra, Keith Baker, Gabriel Spitz, Adam Bailey, Paul Titus, Brian Rubineau, Jason Sidman, Bonnie Baker, Jean MacMillan, Marcus Louie, and Kathleen Carley.

The opinions presented here are those of the author. The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents. Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Abstract

Military operations in urban environments can be characterized as complex systems in which the operation both influences and is influenced by numerous interactions between system components. Consequently, given the level of complexity inherent in urban operations, it is particularly difficult to reason about the potential outcomes of various actions and events. What is needed are analysis tools that effectively embrace the complexity of the urban operational environment. This manuscript briefly outlines the nature of this problem and then reviews one example of a modeling tool that attempts to account for this complexity. The VISualization of Threats and Attacks (VISTA) tool is based on a multi-agent network model that incorporates multiple interacting and adaptive elements (agents) that represent various entities and regions of a city. The modeling tool provides understanding through exploration of the emergent behavior of these agents as they react to events based on their characteristics, history, and connectivity. Through this type of simulation, the VISTA system enables exploration and visualization of the consequences of hypothetical actions and events.

Multi-Agent Modeling of the Urban Operational Environment

Military operations in urban settings are particularly complex due to factors such as a high number of non-combatants, substantial infrastructure, a multidimensional battlespace, and many avenues of approach (Gerwehr and Glenn, 2000). Indeed, urban environments can be characterized as complex systems. Complex systems are those that have many interacting components, such that they exhibit non-linearity and emergent behaviors (e.g., Czerwinski, 1998; Prigogine and Stengers, 1984; Waldrop, 1992). This means that the overall behavior of these systems arises from interactions between multiple components (self-organization). In the case of urban environments, the interacting components range from numerous people to transportation systems to various aspects of the city infrastructure. Hence, military operations in urban environments can be characterized as complex systems, for the operation both influences and is influenced by interactions between a wide-range of system components.

Consequently, given the level of complexity inherent in urban operations, it is particularly difficult to reason about the potential outcomes of various actions and events. These difficulties in reasoning result from numerous interactions that can produce sudden events that can be difficult to track, anticipate, and understand. Accordingly, by themselves traditional methods of analysis used to predict the consequences of various courses of action are not well suited to the urban operational setting and mission effectiveness can be compromised. Alone, these traditional methods simply cannot capture the potential for sudden, non-linear, emergent events.

What is needed, therefore, are analysis tools that effectively embrace the complexity of urban operations. These tools must model the urban operation as a complex system and thereby enable analyses that fully incorporate the potential for unexpected interactions. The purpose of this manuscript is to explore one such approach based on multi-agent modeling techniques (e.g., Carley, 1991, 1999). While such an approach will not enable precise prediction per se, it nevertheless holds the promise of promoting anticipation, or forecasting, of when conditions are right for emergent events. Below, I briefly illustrate the nature of the problem and then outline one potential solution, the VISualization of Threats and Attacks (VISTA) tool, which is currently under development as part of a Phase II Small Business Innovative Research contract with the Army Research Laboratory.

The Problem

There have been and continue to be numerous operations in urban settings, including places such as the former Yugoslavia, Beirut, Hue City, and more recently, Baghdad. Many of these cities have also been the setting for peacekeeping operations, otherwise known as Stability and Support Operations (SASO). An interesting example is the city of Mitrovica in Kosovo. Mitrovica has been characterized by well-defined boundaries between different ethnic groups with a long history of violence. Historically, there has been a Serbian majority north of the River Ibar and an Albanian majority south of the river. However, there have also been concentrated pockets of Albanians, Serbians, and other groups on the "wrong" side of the river. Despite the presence of the Kosovo Force (KFOR), there has been and continues to be various outbreaks of violence in this city, especially along the borders between the distinct city sections.

For instance, according to published news reports, in the year 2000 there were repeated clashes in Mitrovica (BBC, 2000). One set of reports from February of 2000 describes a series of events that led up to the imposition of a curfew after KFOR forces came under direct fire and an ethnic Albanian, described as a sniper, was shot. This followed an earlier set of incidents in which Mitrovica was the site of grenade explosions and weapons fire. Interestingly, and critically, the reports indicated that it was unclear who started the violence, in that it may have been started when a grenade was thrown into an Albanian home, or when several ethnic Albanians from the south side of the river crossed to the north, or when KFOR raided a bar that Albanians claimed was a base for Serbian paramilitaries. Such uncertain causation, or more specifically multiple causation, is a hallmark of complex systems in that no single event preferentially determined the outcome, but rather, the events that unfolded were determined by several interacting factors.

From an intelligence perspective, therefore, such a situation presents a number of interesting, yet daunting, problems: For instance, what effect would the curfew have? Could the escalated violence have been predicted from the grenade attack alone, or did it require an understanding of the composite situation? What friendly courses of action could have been followed to prevent or positively affect the escalating violence, if any? Why do such instances sometimes escalate, while at other times they do not? What might the effect of additional forces be, or of a shortage of clean water or electricity? Clearly, these problems are difficult, complex, and interrelated.

The VISTA Tool

Given this complexity, what is needed to help understand these types of situations is an analysis tool that enables the determination of when conditions are right for emergent events. The VISualization of Threats and Attacks (VISTA) tool is designed to fulfill this need given its basis in complex systems theory. With the VISTA tool, given a certain set of conditions, and a general understanding of the kinds of factors that lead to particular events, an analyst may indeed be able to "forecast" possible future scenarios. Moreover, it might also be possible to explore how to influence conditions by pursuing hypothetical actions such as inserting forces in particular locations or by imposing curfews. When variables like these are manipulated, emerging events may actually become less or more likely as forces within the environment are manipulated. The VISTA tool is designed to support these types of hypothetical analyses. Figure 1 shows a prototype version of the tool interface and illustrates the results of an over-time analysis using hypothetical data.

More specifically, at its core, the VISTA model rests on a multi-agent approach (e.g., Carley, 1991, 1999) that incorporates multiple interacting elements (agents) that represent the entities involved (friendly, hostile, and neutral) and the different regions (neighborhoods) of a city like Mitrovica, where each agent reacts to events depending on its characteristics and its connectivity with other regions/entities. The model focuses on how these agents interact and learn. System behavior emerges from these interactions and it is this emergent behavior that provides predictive power through the exploration of hypothetical events and outcomes.

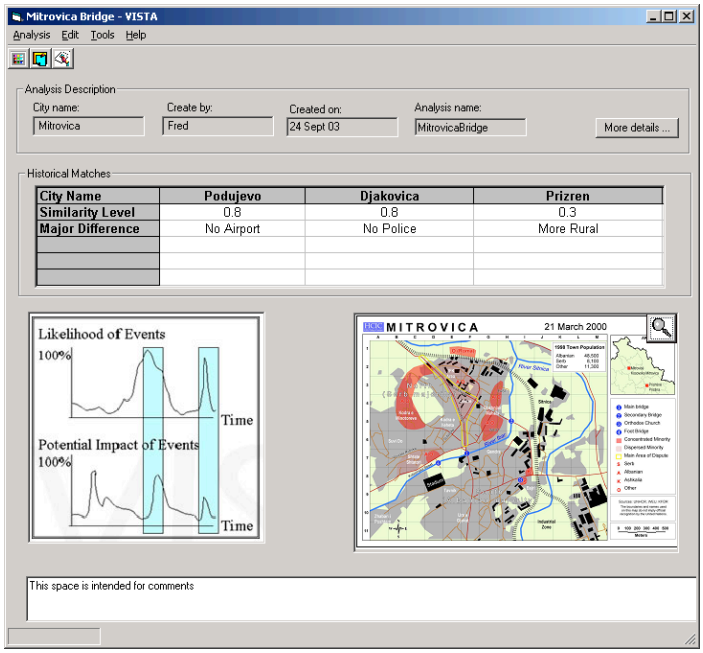


Figure 1. Prototype framework for tool interface.

Figure 2 shows a high level view of the overall framework for the VISTA tool. Referring to Figure 2, there are several key components:

Databases. The system rests on a set of database tables that serve to provide historical context, city characteristics, and entity characteristics. These tables contain information on the current city of interest, including global characteristics and information on particular regions (sectors, neighborhoods) such as the size of the city/sector, population density, poverty levels, and locations of key infrastructure. In addition, the tables contain descriptive information on the various entities involved. Similarly, historical context is provided by database tables on previous events, the cities in which they occurred, and the entities involved (e.g., Hue City, Mogadishu, Beirut).

The City Threat Evaluator. The City Threat Evaluator (CTE) component initiates analyses by providing a method to judge the likelihood of a threat and its potential severity through reliance on data about the city of concern, including items such as the physical, political, economic and demographic layout (as captured in the databases). Based on this collective input, the city evaluator uses an algorithm to predict the potential for threat by using information on the city and the specific entity agents in conjunction with information on historical events to determine the best match. Given a city, the entity agents, and the match, the CTE will generate potential threat level overall and by sector based on association with historical events. This estimate provides the initial conditions for further analyses.

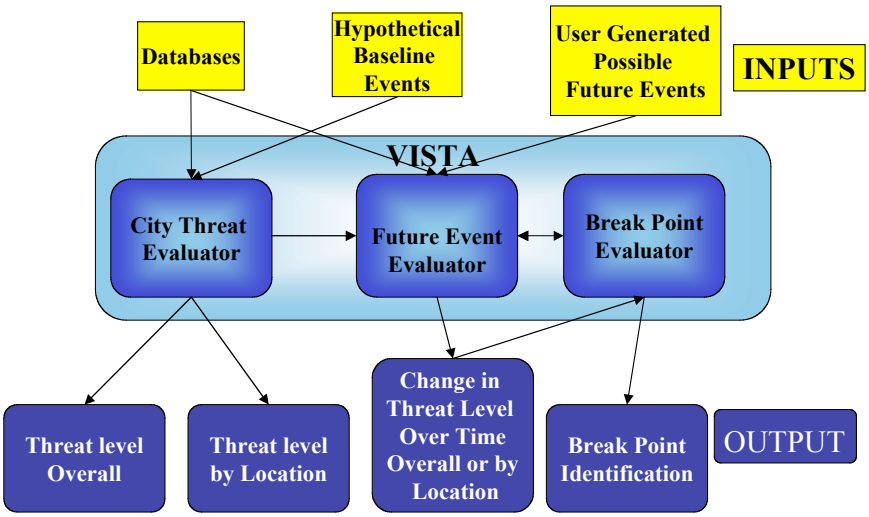


Figure 2. The VISTA analysis tool.

The Future Event Evaluator. The Future Event Evaluator (FEE) component enables the evaluation of "what-if" questions about specific events of interest, including friendly actions (e.g., the imposition of a curfew) and hostile actions (e.g., the explosion of a bomb). This module allows the user to specify possible future events, and, based on complex interactions, it predicts dynamic changes in threat level by time and location. To accomplish this, the FEE employs a multi-agent network that uses data on the city and entities in question, a set of hypothetical events, and previous events to evaluate the likelihood and severity of threat. City sectors are defined as agents based on characteristics of the city, and similarly, entity agents are defined based on their characteristics. These agents are dynamic, in that they learn, adapt, and respond to other agents. The output of the system reflects the patterns that emerge from the interaction of these agents and represents the likelihood of attacks. Consequently, through use of this module in a what-if manner, the analyst can explore the potential consequences of a variety of actions based on the modeled interactions. Figure 3 shows sample data from a prototype version of the FEE. This figure plots sector tension (threat level) over time in nine regions of a hypothetical city and threat (enemy) agent tension (readiness to act) for three hypothetical threat agents. In this example, there are "attacks" at times 3 and 10, leading to changes in tension levels over time based on the multi-agent modeling of system interactions.

The Break Point Evaluator. Building on the FEE, the Break Point Evaluator (BPE) runs a number of what-if analyses through the FEE and maps the relative impact and likelihood of different outcomes under different conditions. Hence, this aspect of the system provides the ability to systematically explore and represent classes of different actions, events, and outcomes, thereby enabling complex analyses of the manner in which different factors can combine to influence the likelihood of future events. This aspect of the system facilitates the construction of different "surfaces" that systematically relate potential outcomes to changes in multiple variables. Thus, by running many different hypothetical situations like that shown in Figure 2, the BPE enables a relatively complex understanding of the composite situation.

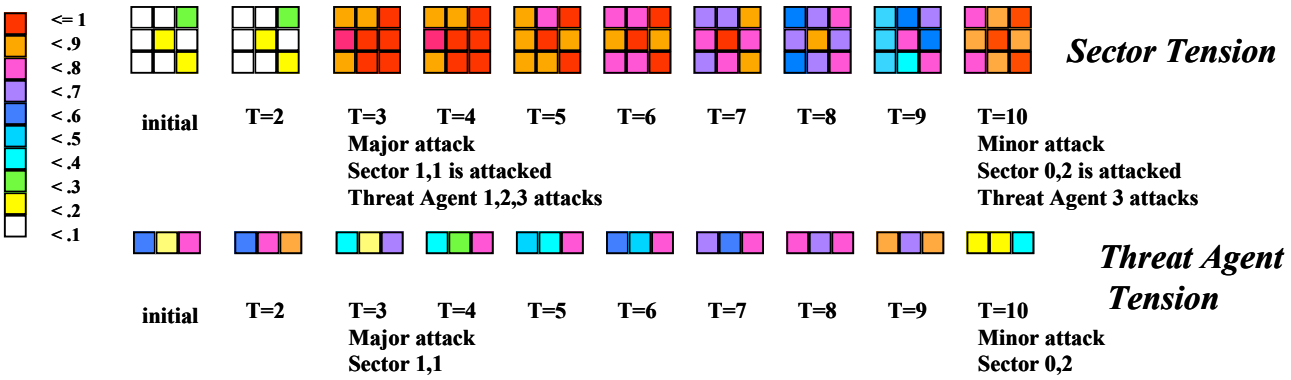


Figure 3. Tension levels over time and by location for a hypothetical city as generated by the FEE modeling component.

Conclusions

As the VISTA example illustrates, it may indeed be possible to harness the power of innovative complex systems theories to better understand urban operational environments. The problem exists because military operations in urban environments both influence and are influenced by interactions between a wide range of system components. It is therefore particularly difficult to reason about the potential outcomes of various actions and events. Consequently, the primary purpose of VISTA is to provide a method that is designed to enable the analyst to better understand how multiple, interacting factors can combine to create unexpected or emergent situations. Without such a modeling tool, it is nearly impossible for the analyst to accurately understand the likelihood and consequences of unanticipated interactions. VISTA addresses this issue by providing a multi-agent based complex systems modeling tool to accurately understand a complex system (the urban operational environment). The tool therefore holds the promise of facilitating the anticipation of when conditions are right for unexpected events, thereby supporting the timely recognition of emerging patterns and opportunities for action.

References

BBC (2000); Mitrovica: Symbol of Kosovo's division; http://news.bbc.co.uk/2/hi/europe/652228.stm

Carley, K. M. (1991); A theory of group stability; American Sociological Review, Vol. 56 (pp. 331-354)

Carley, K. M. (1999); On the evolution of social and organizational networks; Research in the Sociology of Organizations: Networks In and Around Organizations (ed. S.B. Andrews & D. Knoke), JAI Press, Inc.

Czerwinski, T. J. (1998); Coping with the bounds: Speculations on non-linearity in military affairs; National Defense University Press.

Gerwehr, S., & Glenn, R.W. (2000); The art of darkness: Deception and urban operations; (http://www.rand.org/publications/MR/MR1132/)

Prigogene, I., & Stengers, I. (1984); Order out of chaos: Man's new dialogue with nature; Bantam

Waldrop, M. M. (1992); *Complexity: The emerging science at the edge of order and chaos*; Simon & Shuster

ARES Agent Technology Overview

Adam Gray
ARES Agent Team Leader
CDM Technologies, Inc
San Luis Obispo, CA
adgray@cdmtech.com

Abstract

The ARES Team, a development group within CDM Technologies, Inc., applies expert-agent technology to the development of decision-support tools that promote effective planning and coordination in dynamic multi-user environments. The software employs two major categories of agents: subscription-based and rule-based. Subscription-based agents are individual processes or components that operate at the architectural level of the system. Rule-based agents correspond to modules within an expert system shell environment that each contain a rule set targeted to encode a particular area of expertise within the application domain. The use of a java-based expert system shell allows the use of agent resources written in java, such as Bayesian networks, searching and planning, and case-based reasoning facilities, to be used directly within the agent rules. This provides an environment in which multiple Artificial Intelligence (AI) paradigms can be brought to bear on a decision-support problem and affords ARES applications the flexibility required to deal with the complex and dynamic environments that are typically targeted by real-world decision-support systems.

Introduction

CDM Technologies, Inc. applies expert-agent technology to the development of decision-support tools that promote effective planning and coordination in complex multi-user environments. ARES is the development team within CDM Technologies responsible for the following successive series of agent-based decision support system prototypes sponsored by the Office of Naval Research (ONR): the Collaborative Infrastructure Assessment Tool (CIAT), the Collaborative Agent Based Control and Help System (COACH), the Ordnance Tracking Information System (OTIS) and the Shipboard Integration of Logistics Systems and Mission Readiness Assessment Tool (SILS-MRAT). This paper describes some of the approaches and technologies used in the development of these and other systems by the ARES team.

ARES agent technology is based on the Integrated Cooperative Decision Model (ICDM) development framework (Pohl, 2002). ICDM consists of an underlying architecture, fundamental design criteria, and development tools and processes for creating agent-based decision-support systems. The underlying architecture provides a set of high-level application-independent subsystems and the mechanisms to support collaborative interaction among them. These generic subsystems can be quickly tailored to produce an application specific architecture and implementation utilizing the ICDM development tools. The initial development of ICDM was undertaken by the Collaborative Agent Design Research Center (CADRC) at California Polytechnic State University, San Luis Obispo. Based on a three-tier architecture, ICDM incorporates technologies, such as distributed-object servers and inference engines, to provide a

collaborative environment for agent-based decision-support systems that provides both developmental efficiency and architectural extensibility.

The agents employed by ICDM are software processes, components, or modules that have the ability to perceive the external environment and autonomously act on it in collaboration with other agents. Agents act in a manner conducive to achieving the individual and collective goals of the system and users. The external environment in which agents are situated is both bounded and defined by the ontology they employ to interact with it. The ontology provides a vocabulary to describe the external environment that is constrained in accordance with the underlying principles operating in the environment, such as the physical laws that constrain our own environment. The ontology allows agents to express their specific interests in an environment, communicate their conclusions about it, specify actions on it, and record knowledge about it.

ICDM based software employs two major categories of agents: subscription-based and rule-based. Subscription-based agents are individual processes or components that operate at the architectural level of the system. Rule-based agents correspond to modules within an expert system shell environment that contain rule sets targeted to encode particular areas of expertise within the application domain. Both categories of agent are proactive in that they automatically act in response to changes in the virtual representation of the external environment and therefore do not have to be explicitly told to act as is done in traditional procedural paradigms.

Subscription-Based Agents

Subscription-based agents use the standardized Common Object Request Broker Architecture (CORBA) services that the ICDM runtime environment provides along with a proprietary subscription service to register their individual interests within the domain. The ICDM Subscription Service alerts individual subscribers to changes in the collection of distributed objects used to represent the domain, which satisfy their registered interest, by pushing the changes to the corresponding subscriber. This capability, by allowing the sharing of a single executable ontology between multiple processes, allows the individual agent subscribers to collaboratively interact without any prior knowledge of each other in an efficient and scalable fashion. This subscription-based collaboration can be seen in Figure 1 where multiple agent-based systems are shown subscribing to and sharing information from a single, albeit distributed, ontology.

Rule-Based Agents

Subscription-based agents may in turn contain rule-based agents that operate in modules within the parent process or components that maintain the associated agent subscriptions. Rule-based agents utilize specialized declarative languages to precisely specify a state in the external environment and the action that should be performed when the specified state is observed. They work at a much lower level of granularity than that employed by subscription-based agents. This level of granularity requires specialized data structures and algorithms to efficiently match on the states of the external environment. To date the required level of efficiency is only found in Rete Algorithm based expert system shells (Forgy, 1982). The traditional problem with expert system shells is that they are stand-alone development environments that do not interoperate with the general-purpose environments required for graphical user interface (GUI) development or for relational database interaction.

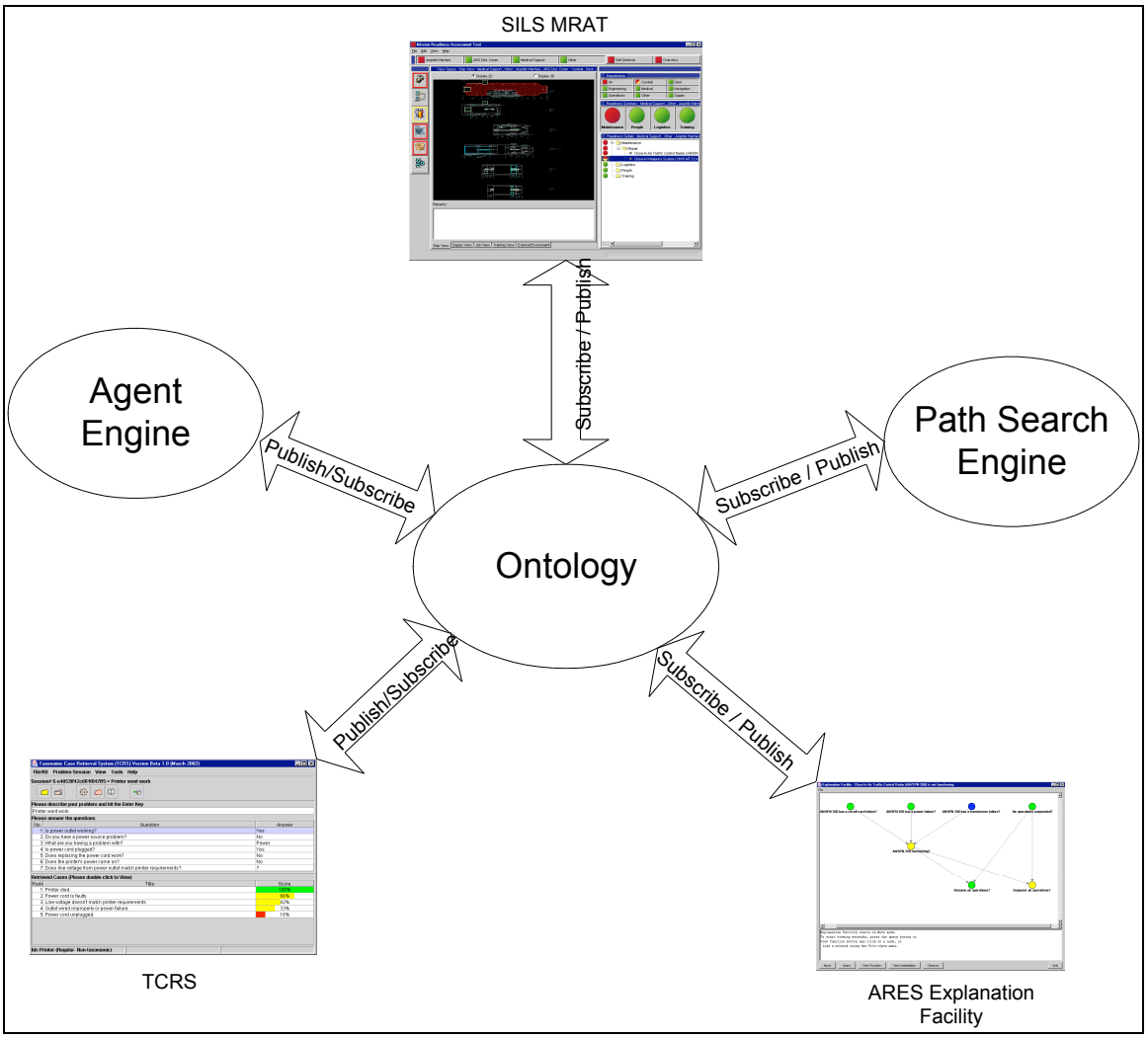


Figure 1 - Subscription-based agent interaction

Interoperability with expert system shell environments is a core technological feature of ICDM-based applications. This interoperability is provided through proprietary adaptations to existing expert system shell environments that enable them to seamlessly operate as plug-in clients to the distributed ICDM Object Serving Communication Facility that houses the virtual representation of the external environment. Additional extensions have also been created to better manage the distribution of processor time between the resident agent rule sets.

Traditionally, rules written in rule-based agent technologies have required the inclusion of objects that have necessary information for rule action but are not directly involved in the pattern that triggers rule activation. As this approach forces a larger number of objects to be maintained within the Rete network it can lead to significant performance degradations. The ARES team has worked to keep all object detail not involved in the triggering of rules out of the rule activation patterns associated with the Rete network by directly utilizing the query capabilities provided by ICDM in the action portion of the rules. Objects that are not directly involved in triggering the

activation of a rule are now queried for on demand and then released. This approach has had a significant positive affect on the performance of ARES ruled-based agents in the context of realistically sized data sets.

The use of Jess, a java-based expert shell environment, by the ARES Team has allowed agent resources written in java, such as the graph library and case-based reasoning engine, to be used directly within the agent rules; thereby providing an environment in which multiple AI paradigms can be brought to bear on the decision-support problem. Some of these java-based agent resources, as well as the progression of agent-based approaches that led to their development, are described in the following sections.

Inference Approach

Earlier agent-based systems implemented by the ARES team have been comprised of a knowledge base containing accumulated experience and a set of rules for applying the knowledge base to each particular situation that is to be addressed by the program. While this approach works well in systems with static rules that contain no uncertainty it quickly becomes insufficient as complexity increases. These types of systems require frequent updates as the developers of the system must add the new knowledge. Furthermore, learning techniques, defined as the ability to modify agent behavior without developer intervention, are not well supported, as the system cannot dynamically incorporate new knowledge at runtime.

The ARES team addresses these issues by employing observation-based inference. This approach entails the representation of the majority of operational information within the system as observations. Each observation has a knowledge-level concept and the relationships between these concepts form the basis for agent inference. Agent rules look for generic patterns between concepts and infer new observations and alerts based on logical (and, or) patterns between them. This allows users of the system, or agents within the system, to dynamically add concepts and concept relationships. It also creates a foundation for learning that had not existed in earlier systems. However, as the system rarely has access to all relevant information, there are few situations in which an inference can be made with 100% certainty. Thus, it is advantageous to provide a user with the most likely inferences and their appropriate probability of truth. The ARES team is addressing this issue through the development of Bayesian Network reasoning facilities and the incorporation of probabilistic elements in our core ontology.

Bayesian Networks

A Bayesian network, or belief network, is a causal graph, associated with an underlying distribution of probability (Norvig 2003). Each leaf node within the graph contains a prior probability table and all other nodes contain a conditional probability table relating it to connected nodes (Figure 2). This representation expresses all the information contained within a joint probability distribution yet in a much more concise format. The inherent advantage of these graphs is that the probability of any given output variable can be determined without knowledge of all the input variables.

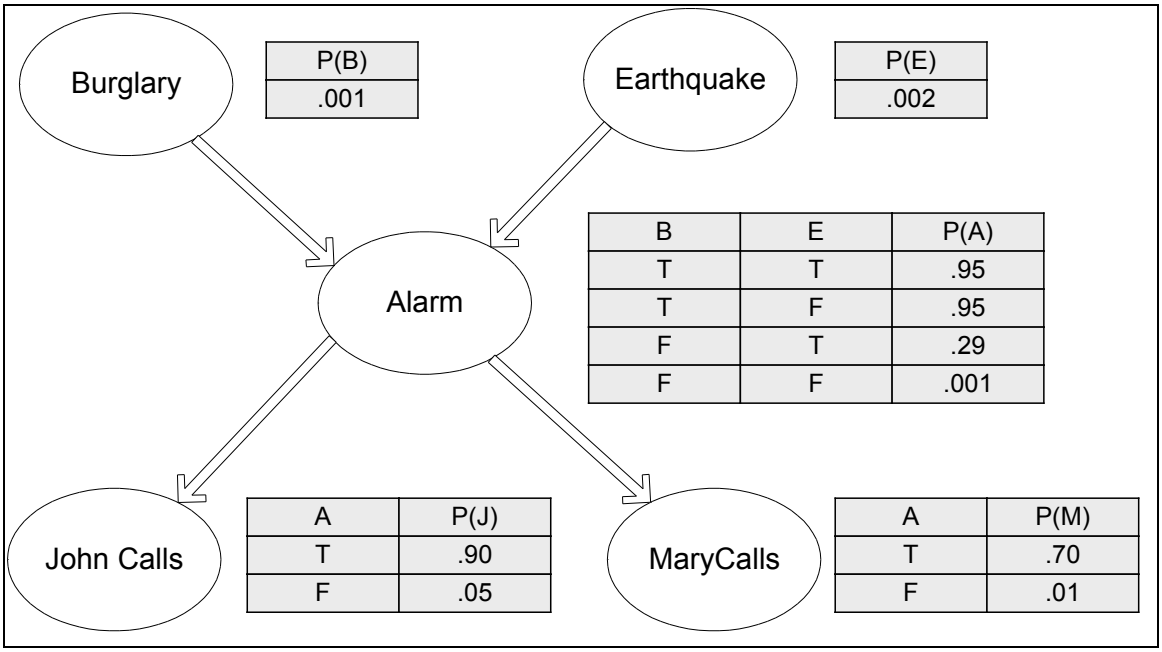


Figure 2 - A typical belief network with conditional probabilities.

Another advantage is that past operational data can be easily incorporated into the knowledge base as probabilities can be determined by a combination of these prior data and/or human prediction. This also allows an intuitive and computationally sound vision of learning as new data can be dynamically used to recalculate the network probabilities.

Implementing Bayesian networks for use by agents within such systems has some inherent difficulties. A conditional probability table is difficult to model in an object-based format without necessitating a large number of objects. This is especially the case in belief networks with probability nodes influenced by more than two other nodes or that contain probability nodes with more than two variables. The number of objects necessary to represent a Bayesian network is on the order of $\Omega(n * v^k)$ where n is the number of nodes, v is the number of variables per node and k is the number of nodes that directly influence each other node. As there is an exponential relationship between the number of necessary objects and the number of nodes directly influencing each other node, the number of objects can become large very quickly. However, this representation is significantly more efficient than the use of a full joint probability distribution. Consider a network with 20 nodes $(n = 20)$, 5 parents per node $(k = 5)$ and 2 Boolean variables $(v = 2)$, the Bayesian network requires approximately 640 objects while the full joint probability distribution requires over a million nodes.

Adding Bayesian Network technology to an agent-based system also has the difficulty of handling context within a given decision-support system. For example, if a query is made for the value of the probability variable "Person is sick" the system must query a network with only the observed concepts directly relevant to that person. Hence, a network must exist for each set of

conflicting operational data. Depending on the amount of conflicting data for a given system this can have considerable memory and performance impacts.

Bayesian Network technology used within ARES applications can be viewed through the ARES Explanation Facility shown in Figure 3. The Explanation Facility presents a graph-based view of both the structure and current probabilities of a belief network. This allows an in depth description of the current state of the system as well as an intuitive explanation of the logic associated with a specific agent observation inference. The evidence leading to an inference can be easily determined as the nodes are directed and colored based upon state. Nodes are green by default, blue when observed, and yellow when inferred by the system. Inferences are made based on a degree of belief threshold set for each probability variable by the designer of the belief network. For example, a network designer may specify that a user alert be created when there is a degree of belief greater than 50% that an engine will overheat. This threshold specification allows dynamic user customization of system inference and resulting alerts. A user may also experiment by virtually observing nodes within the Explanation Facility and viewing the resulting probabilities, and inferences, without affecting the actual state of the system.

Graph Library

The ARES agents may also make use of a graph library and accompanying set of classical search algorithms, developed for use within the Jess environment. The library allows simple java-based construction of a directed graph of vertices and weighted edges that may include self-loops. A hybrid of an algorithm developed by David Eppstein at the University of California Irvine may be used to determine a specified number of ordered shortest paths between any two terminals over the constructed graph (Eppstein 1997). These k shortest paths can be found in a graph with n vertices and m edges in time $\Box(m + n * \log(n) + k * n)$. Dijkstra's well-known algorithm is used to calculate the single shortest path for a given graph and runs in time $\Box((m + n) * \log(n))$ (Eppstein 1997).

ARES employs a Path Search Engine developed on top of the graph library that allows querying for shortest path results by any application subscribing to the ICDM Subscription Service. It requires the creation of a path query object, containing the start and terminal nodes as well as the number of paths requested, to notify the search engine of the desired query type and the number of results. The Path Search Engine then generates the requested number of shortest paths from the constructed graph and associates a path object to the query object for each result. This allows multiple agent-based processes to share and collaborate upon results from a single query (Figure 4).

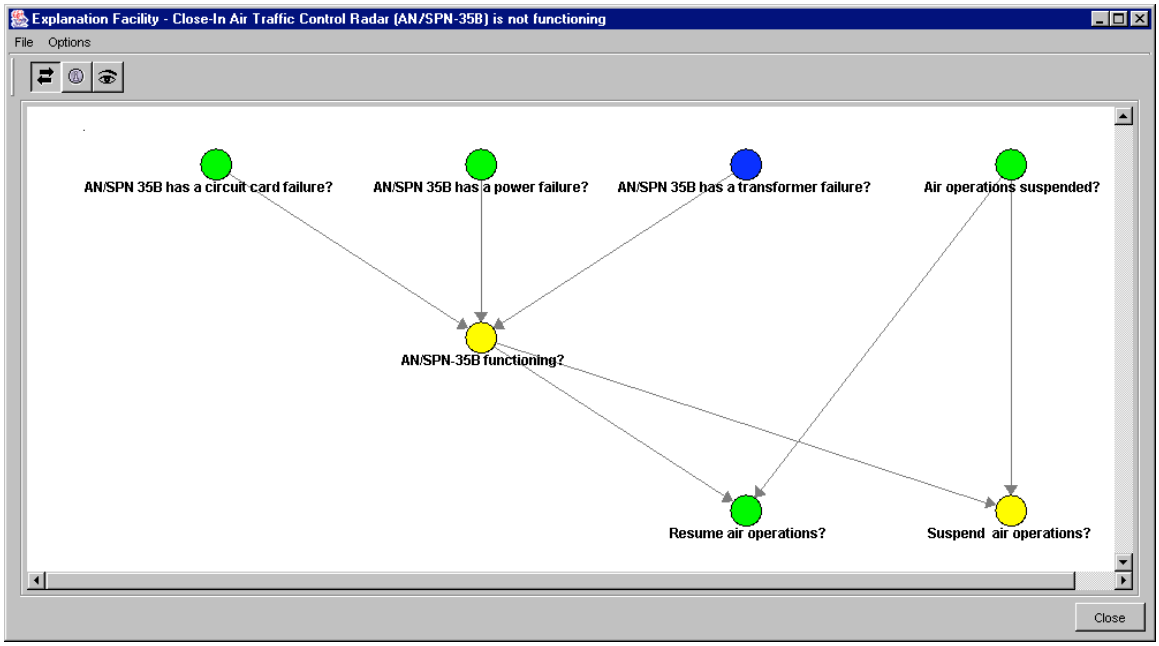


Figure 3 - ARES Explanation Facility

Case-Based Reasoning

Ares employs TCRS v1.0 (Figure 5), a taxonomical conversational case-based reasoning system developed at the Naval Research Laboratory (Aha and Gupta 2002). TCRS supports problem solving by recalling and applying past experiences, or cases, that are similar to the problem at hand. It allows a user to incrementally specify a query by providing text annotations and answering prompted questions. This query is combined with answered questions and the result is matched against previous cases to determine the most similar past experience. The similarity measure between two text strings is calculated using the different trigrams in the two strings as shown in Equation 1 where *tri(x)* is the set of trigrams in x. For example *tri(eloquent) = {elo, loq, oqu, que, ent}*.

$$sim(x, y) = 1 \Big/ 1 + |tri(x)| + |tri(y)| - 2 * |tri(x) \cap tri(y)|$$

Equation 1 – Similarity measure between two text strings x and y

TCRS features taxonomical relationships between cases to help handle the abstraction difficulties inherent in applications targeted by conversational case-based reasoning systems. For example:

(1.) The weather was bad
  (1.1) The weather was stormy
    (1.1.1) The wind speed was very high
      (1.1.1.1) The wind speed was over 90 mi./hr

would be represented in a hierarchical structure of cases within TCRS. This makes the case representation more efficient as it is indexed by fewer and only the most specific question-

answer pairs available at the time of indexing, it also eliminates any unwanted correlation among features that could result from inherent abstraction and it makes the conversation responsive to the level of abstraction in a user's query, which can be correlated to the user's level of expertise in a particular domain.

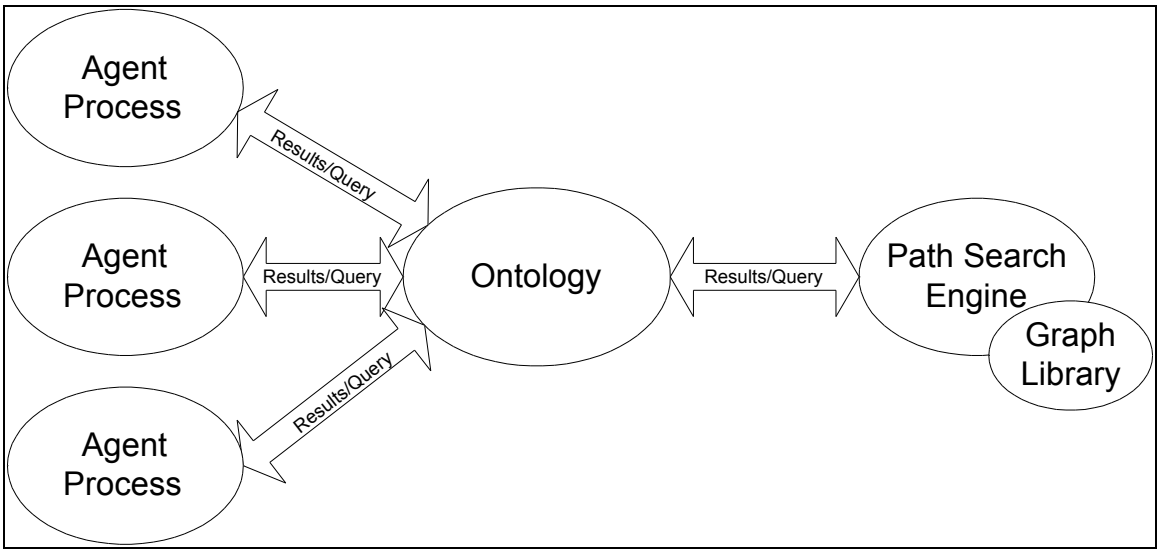


Figure 4 - Path Search Engine interaction

Figure 5 shows the TCRS application loaded with an example case base from the printer-troubleshooting domain. A text field is provided to enter in a description of the user's problem. The top table displays currently answered questions as well as a ranking of unanswered questions most likely to assist in the determination of similar past cases. The bottom table shows the currently ranked past cases with their percentage of similarity to the original text string and answered questions. The actions most commonly performed in response to a past case may be displayed by user selection of the retrieved case's row.

Summary

Built upon the distributed-object architecture provided by ICDM, the ARES team provides a toolkit in which software agents collaboratively employ multiple AI paradigms in response to a given problem. The toolkit's Bayesian Network technology provides observation-based inference in uncertain environments as well as dynamic learning through probability recalculation. Case-based reasoning tools within the toolkit provide ranking of possible courses of actions through analysis of previous experience. A path search engine and accompanying graph library are also included and allow efficient multiple-result searching and planning on an object-based graph. The ability to bring any number of these solutions to bear upon a given problem provides ARES applications the flexibility required to deal with the complex and dynamic environments typically targeted by real-world decision support systems.

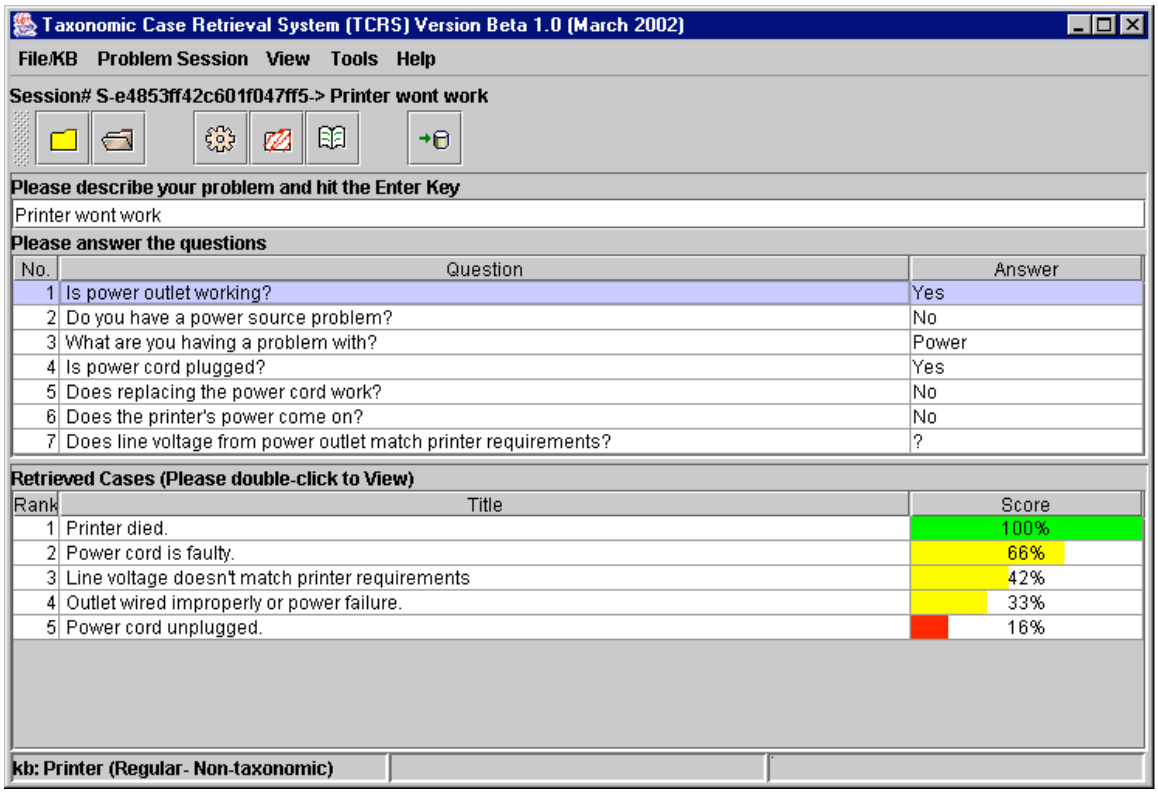


Figure 5 - TCRS v1.0

References

Aha, David W. and Gupta, Kalyan Moy (2002), *Causal Query Elaboration in Conversational Case-Based Reasoning*; Proceedings of FLAIRS'02.

Eppstein, David (1997), *Finding k-Shortest Paths*; Department of Information and Computer Science, University of California, Irvine, CA.

Forgy, C. (1982), *Rete: A Fast Algorithm for the Many Patterns/Many Objects Match Problem*; Artificial Intelligence, Vol. 19 (pp. 17-37).

Gupta, Kalyan Moy (2001), *Taxonomic Conversational Case-Based Reasoning*; Proceedings of the fourth ICCBR, D. W. Aha & I. Watson (Eds.), Springer, Berlin, Germany, pp. 219-233.

Koller, Daphne, Avi Pfeiffer (1997), *Object-Oriented Bayesian Networks*; Proceedings of the Thirteenth Conference on Uncertainty in Artificial Intelligence.

Pohl, K. (2002), *The Underlying Design Principles of the ICDM Development Toolkit*; InterSymp-2002, Focus Symposium on Collaborative Decision-Support Systems, Baden-Baden, Germany, July 30 (pp. 51-8).

Russell, Stuart, Peter Norvig (2003), *Artificial Intelligence A Modern Approach 2nd Edition*; Prentice Hall, Englewood Cliffs, NJ.

Zang, Michael A., Chris K. Neff (2003), *SILS MRAT: A Shipboard Integration of Logistics Systems and Mission Readiness Assessment Tool*; Thirteenth International Ship Control Systems Symposium (SCSS), Orlando, Florida.

Zang, Michael A. (2003), *The Knowledge Level Approach To Intelligent Information System Design*; Collaborative Agent Design Research Center, Cal Poly San Luis Obispo, Ca.

Ontological Approaches for Semantic Interoperability

Michael A Zang
Technical Leader
CDM Technologies, Inc.
mzang@cdmtech.com

Abstract
This paper provides a basic description of the concept of an ontology. It then describes how ontologies are structured and employed in the context of interfaces between software based information systems. This usage is discussed in the context of three successive levels of semantic interoperability between two example systems. The paper goes on to suggest that the interfaces between information systems should perhaps be viewed and implemented as systems themselves. The paper concludes by providing a brief summary of what was discussed.

Keywords
Agent, Data, Information, Interoperability, Knowledge, Object Model, Ontology, Semantics

Introduction
An ontology is an explicit specification of a conceptualization. The term is borrowed from philosophy, where an ontology is a systematic account of existence. For a software application, what "exists" is that which can be represented. When the information and knowledge of a domain is represented in a declarative formalism, the set of objects that can be represented is called the universe of discourse. This set of objects, and the describable relationships among them represents all the information and knowledge that can be known in the context of the applications that employ them. In such an ontology, definitions associate the names of entities in the universe of discourse (e.g., classes, relations, functions, or other objects) with human-readable text describing what the names mean, and formal axioms that constrain the interpretation and well-formed use of these terms.

In terms of semantic interoperability, an ontology defines the vocabulary with which queries and assertions are exchanged among applications. Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner. The applications sharing a vocabulary need not share a knowledge base; each knows things the other does not, and an application that commits to an ontology is not required to answer all queries that can be formulated in the shared vocabulary.

An Interface Domain Ontology is an ontology specifically geared towards interfacing multiple domain specific software systems. The concepts in an Interface Domain Ontology can be organized in a hierarchical structure of three layers as shown in Figure 1. In the Upper Level Ontology are generic concepts, such as 'process', 'agent', 'set', ‘proposition’, and 'goal'. In the Lower Level Ontology are the elementary concepts, such as 'SSN', ‘NEC’, 'street number', 'cost' and 'internet Address'. Generally, for two cooperating partners, it is relatively easy to reach a consensus on the concepts of these two parts especially if they both operate within a common overarching domain such as the Department of the Navy, which provides for common terms and

concepts. The difficult section is the Application Level Ontology. The concepts defined at this level depend strongly on the specific application domains to be encompassed by the interface, which dictates the kind of problems to be addressed, the method used to solve them, and the underlying technology which often contaminates the model of a particular application domain. Typical concepts in this layer are 'supply requisition', 'maintenance action', 'efficiency rating', and ‘reliability index’.

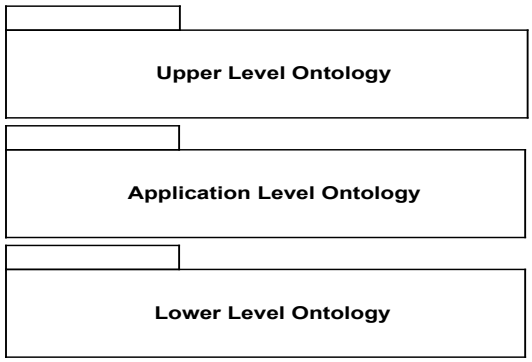


Figure 1: Ontology Semantic Levels

Interoperability Example

In order to better understand these concepts a simple example is in order. This example considers the relationships between supply and maintenance activities and the corresponding information systems that support them. Assume the supply and maintenance systems were initially developed in complete isolation from one another with the respective goals of automating the internal processes of the supply and maintenance departments. These processes were based on the flow of standardized paper forms through the various sections of the two organizations. The forms are delivered to inbox of a particular section whose members typically perform some real-world action that is recorded on the original form or on a new form resulting from the action. These records are then placed in the outbox of the section to begin the next leg of the journey specified by the department process. The automation provided by the information system of each of these two activities essentially mirrors the respective manual processes but replaces the physical entities of the process such as paper forms and in/out boxes with virtual representations that exist only within the confines of a computer.

Additionally assume that automation provided by these systems is internal to the corresponding activity, which requires the generation of physical artifacts to interface with dependent activities. The maintenance activity produces paper based supply requisitions for delivery to the supply activity, which acts to fulfill the request eventually producing a paper based shipment order that is returned to the maintenance activity indicating the requested physical parts that are to be delivered. Maintenance system users that wanted to know the status of their shipment would contact Supply Department personnel by phone. Supply personnel would then query the system to provide a verbal status report to the Maintenance Department caller.

Internal to each of these activities, many other types of documents, and tables are employed to manage them such as maintenance and delivery schedules, shipping rates, and trouble-shooting protocols. In ontological terminology these two different sets of entities and artifacts are known

as domains, which this example further specifies as the Maintenance Domain, and the Supply Domain. For the purposes of this discussion these domains can be thought of as having three layers. The semantic layer describes the structure of the domain entities and the relationships between them that together comprise a model for representing the corresponding real-world problems within the computer. This is a conceptual layer that is somewhat independent of the physical implementation.

The data or information layer contains specific instances of the semantic layer entities linked together in a manner that describes the complete contextual state of a given domain. This is a physical layer that requires a specific implementation paradigm. The entities and relationships defined in the conceptual layer may manifest themselves as linked class instances in an object-oriented paradigm or as related table records in a relational paradigm. The Agent layer contains the domain users and software agents that leverage the information layer to perform useful tasks. The data and information that flows between these domains can be called the Maintenance and Supply Interface Domain or just Interface Domain for short. The Interface Domain is the focus of this paper and subsequently of this example.

As both the example systems evolve and the internal automation is nearing completion or is at least well understood, it is natural that they look to extend the automation across the activity boundaries. In the proceeding sections this paper will use the domains and layers just described to present three successive levels of system to system interaction: Data Level System Interface, Information Level System Interface, and Information Level System Interoperability to characterize different ways in which this automation could be realized.

Data Level System Interface

A data level system interface is characteristic of most of the interfaces between DOD systems at the present time. As the information to be exchanged enters into the interface domain, it looses most context because this type of interface views each exchange as unrelated chunks of data. In this case assume supply system developers are responsible for developing an interface to the maintenance system to periodically pull supply requisitions and the maintenance system developers are responsible for developing and interface to obtain supply shipment status information as requested by maintenance system users. Each group of developers design a record set for the required data, which together define the interface specification that is depicted in Figure 2.

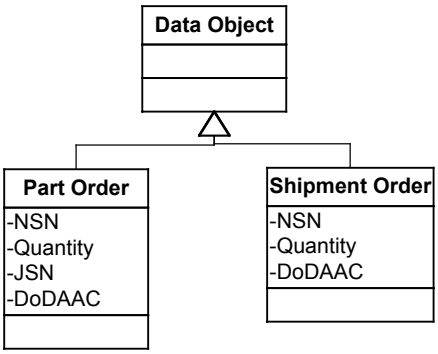


Figure 2: Data Level Interface specification

Although the focus of the interface was the exchange of data rather than semantic content, there is still an ontology associated with the interface. The explicit record specifications (Figure 2) represent the application level of interface domain ontology for the example interface. Most of the attributes found in the record specifications are referenced to entries in the Defense Data Dictionary System (DDDS), which in this case serves the role of the Lower Level Interface Domain Ontology. By marking up the interface attribute definitions in terms of DDDS entities one can easily determine that NSN is the National Stock Number, JSN is the Job Serial Number, and DODAAC is the Department of Defense Activity Address Code. One can reference these in other documentation and data specifications to further ascertain the conceptual meaning associated with them.

While there is no explicit Upper Level Domain Ontology there is an implicit one, which greatly assists developers in finding the common ground to implement this interface. This upper level ontology is an implicit artifact of the standardized processes of the underlying domain, the Department of the Navy in this case, which defines common conceptual entities such as a Maintenance Action Form and a Supply Requisition Form. These common conceptual entities in combination with the attributes defined in the DDDS provide the developers of the two information systems a common vocabulary with which to discuss, design, and develop specific interfaces between their respective systems.

At this point the Semantic Layer of the Data Level System Interface has been defined and is depicted as the Part and Shipment Interface Specification in

Figure 3. The Semantic Layer depicts the internal data models of the Supply and Maintenance domains as well but these fall short of an ontology or even of a specification because they are considered the private proprietary property of the individual organizations responsible for developing the respective systems. It is also likely that these internal models are more focused on the individual forms and tables that users want to appear on their screens rather than on the underlying semantic entities the screens were designed to display information about. This makes it difficult to understand the models outside the context of the applications they were designed to support. While the interface specification appears well defined, the context from which the data is extracted on one end of the interface and then inserted on the other is not addressed by the specification at all.

The Data Layer of the Data Level System Interface realizes the interface specified in the semantic layer. In the case of this example, the maintenance system developers must be responsible for developing the report generator code that pulls the requisite data from the context provided by the maintenance data model to generate the list of part orders that constitutes the interface to the supply system and for developing the report translator code that translates the part shipment interface records into the context of the maintenance data model. Similarly, the supply system developers must be responsible for developing the report generator code that pulls the requisite data from the context provided by the supply data model to generate the list of part shipments that constitutes the interface to the maintenance system and for developing the report translator code that translates the part order interface records into the context of the supply data model. Neither group of developers is really sure how the other group generated the data they

need nor are they sure of what the other group does with the data they generate as they have no visibility into each others data models. The report translators and generators depicted on the figure are representative of these hidden context shifts into hidden proprietary data models.

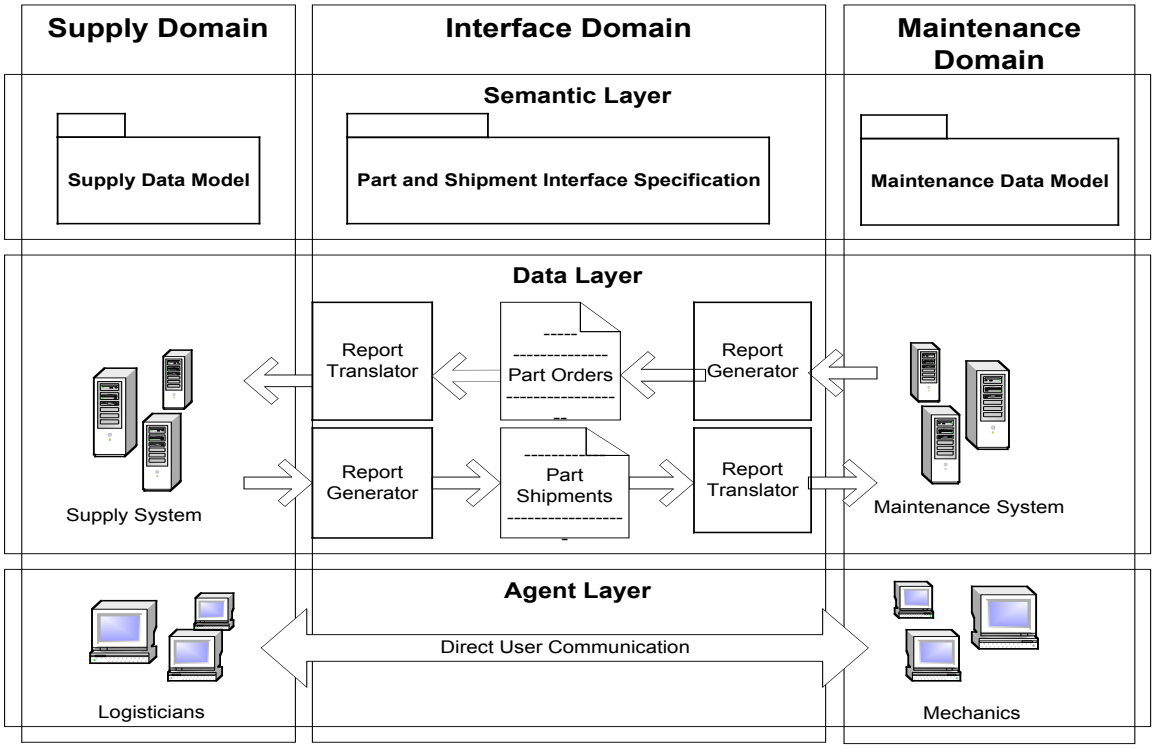


Figure 3: Data Level System Interface

As data level system interfaces such as that described in this example go to the field problems often arise. Since developers are often guessing about the context on either end they often don't quite get it right. This requires the Logisticians and Mechanics that use the systems to perform in the field work-arounds to such as additional filtering or hand tweaking to the records generated from the external system before processing them. Users of these types of data centric systems are use to this sort of data massaging and their systems are well suited to this as the meanings of fields in a data level system are easy to use in locally defined ways; of course this further complicates the problem, as these sorts of local modifications require local tweaks to the interfaces and ultimately produce an interface that marginally accomplishes the intended purpose, is not well understood, and is brittle and difficult to maintain as the corresponding systems evolve.

Information Level Interface

An information level interface differs from a data level interface in several regards. Primary among these is the requirement for the systems being interfaced to be information centric rather than data centric. Information centric systems are based on explicit ontologies that model the underlying semantic entities of the domain rather than the data crunched by the currently favored domain processes or displayed on the screens of particular applications. The developers of an information level interface consider all the information to be exchanged (parts and shipments in

this case) in a singular context which not only relates the entities to be exchanged to each other but to the context in which the entities are related at both ends of the interface. This is show in Semantic Layer of the Information Level System Interface depicted in Figure 4 by an Interface Ontology that overlaps into the Supply and Maintenance Domains. The Interface Ontology is marked up in terms of the shared (public) Supply and Maintenance ontologies and vice versa.

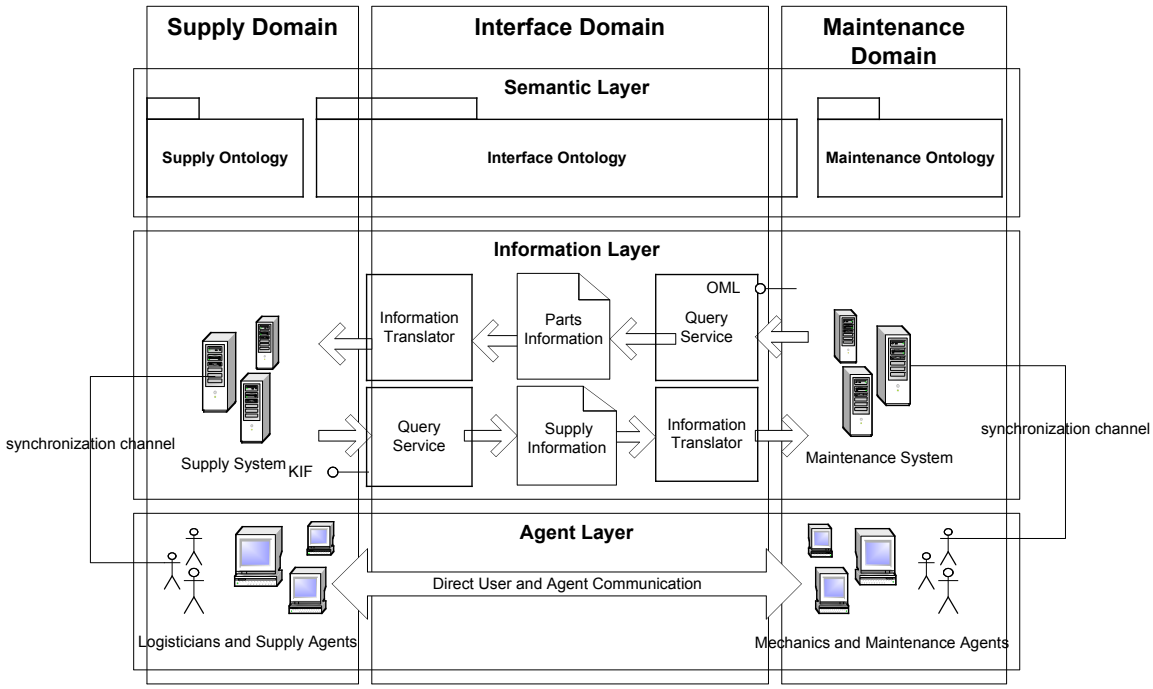


Figure 4: Information Level System Interface

The interface ontology itself will now consist of multiple interrelated entities derived from a Upper Level Interface Domain Ontology that provides higher level semantic context to each entity type concretely defined and used in the interface proper. The Interface Ontology should also define the entities required to pull the interface information from the context of one system and to place it into the context of another, although these constructs may not be present in the physical implementations that transport the information from one system to another it is important that they are defined in the ontology to fully capture the semantic context of the information. The Upper Level Interface Domain Ontology may have existed prior to the development of the interface or may have been developed in conjunction with it. In either case it is important that the application level ontologies specific to the individual Supply and Maintenance Domains in turn utilize it directly or at least reference it by semantically marking up the entities in the ontologies of these domains to correlate them to the concepts defined by the Upper Level Interface Domain Ontology.

With a semantic layer thus defined the information level interface can do much more than generate simple fixed reports. Each system can expose a much more generalized query interface. The queries are formulated and the responses returned in terms of the entities defined in the interface domain ontology. This allows for a much more flexible interface that is more likely to survive evolving interface and system requirements over time. Note that in order to support a

generalized query interface at least one additional interface ontology must be defined that defines the semantics of the queries, or commands that in turn uses the interface domain ontology as logical arguments. For this purpose, many well defined standards exist such as Structure Query Language (SQL) and Knowledge Interchange Format (KIF), or systems may expose their own proprietary but publicly defined interface such as the Object Management Layer (OML) employed by many of the systems developed by CDM Technologies.

Between the information and agent layers in Figure 4 are depicted synchronization channels. In this example the Maintenance and Supply systems are information centric systems that provide for the development of software agents by providing subscription services to client applications. A subscription service is key to agent development as it lets agents register for the ontological patterns that trigger it to action. In this manner agents can always be operating in support of their users, as they are always ready to act in fulfillment of their responsibilities without having to perform needless busy work querying the information store for conditions that may never arise.

Information Level Interoperability

The Information level interface of the previous section has a shortcoming in that the Supply System and Maintenance system must both explicitly query each other to receive new information. Whether or not any new information is available a query must still be run just to find out. On the flip side, immediately after a query has been run information could change in the source system that would not be reflected in the querying system until after processing the next query which may take awhile depending on the polling scheduled employed. This situation can be remedied by employing the same sort of synchronization channel used between the individual information centric systems and the agents they support that is show in Figure 5. The addition of a synchronization channel for the interface allows for the development of interface brokers. Interface brokers serve as agents in the systems they support by automatically synchronizing the state of the system to the state of interest in an external system via the defined interface between the systems.

This approach allows for true interoperability between the systems but is not without its own difficulties. Many of the entities exchanged between the systems correlate to items in the real world and thus have unique identities whose keys must be managed within the confines of a real system implementation. In this sort of information level interface this is typically accomplished by designating a single specific source for each type of unique entity. While this approach works well for interfaces in which only a few systems are participating in starts to break down in larger interoperability scenarios as each system broker must know about all the other systems participating and which system is designated to be the definitive source of which data. This approach requires much duplication of effort within the individual data brokers and introduces an undesirable coupling between the systems. One approach for dealing with this is the introduction of an interoperability server.

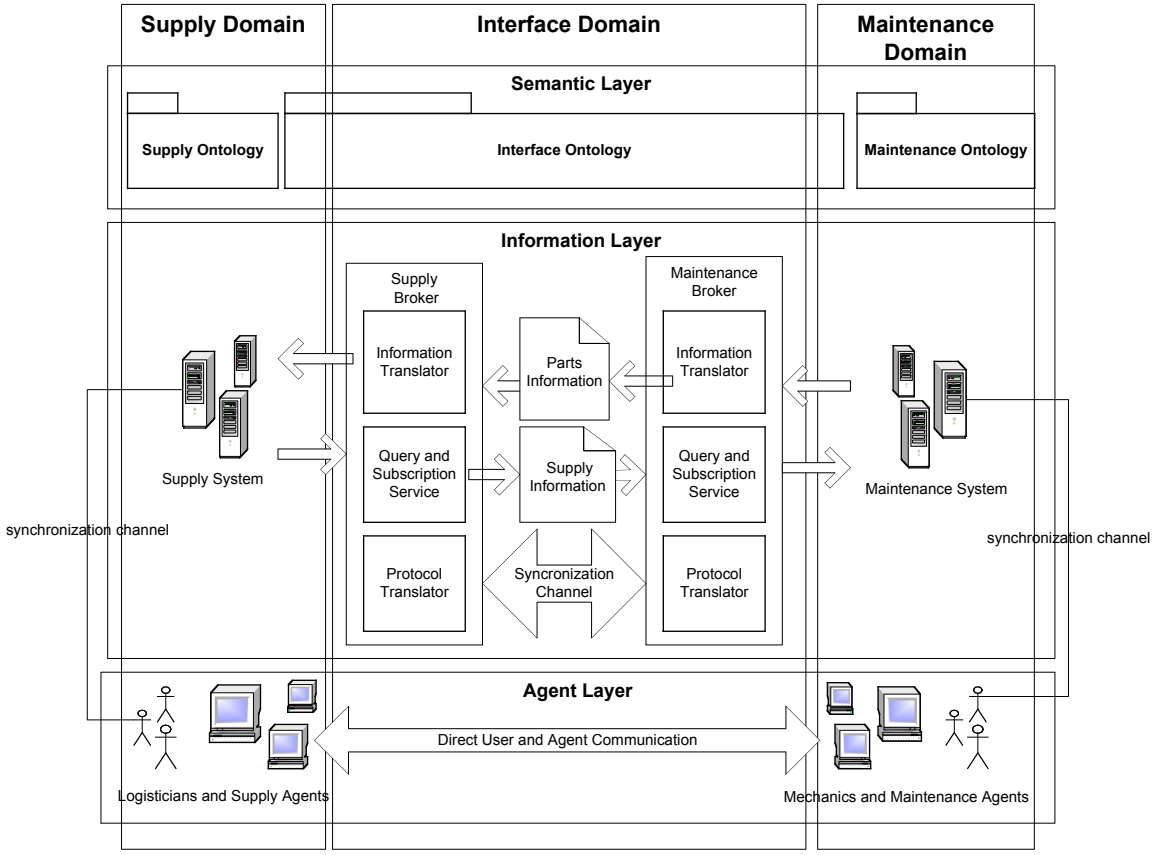


Figure 5: Information Level System Interoperability

Interoperability Server

An interoperability server elevates the interfaces between systems to the level of information centric systems themselves. This approach provides one common implementation of the individual system data brokers that know in which system or combination of systems to find information defined within the Interface Domain Ontology. It also provides specifically for the management of unique entities that are shared across two or more of the interfacing systems.

Employing the concept of an interoperability server leads to a system of systems architecture that groups collections of systems that need to regularly exchange information into loosely coupled federations whose central hub consists of an specific instance of an agent based interoperability server that is configured to address the specific needs of the federation. This concept views the interoperability server as just another system which allows one to layer a hierarchy on this system of systems architecture where higher level federations may include as systems zero or more interoperability servers typically from lower level federations. Within the defense domain, one could envision the proposed system of systems hierarchy following along the lines of existing unit hierarchies within the individual services with a the top level of the hierarchy operating at the level of the joint chiefs of staff, and commander in chief. Of course, crossties between the individual units and services at the lower levels of the hierarchy may also exist. The end state of this vision is a single, albeit large and distributed, system of systems that incorporates the entire information infrastructure of the DOD. This system of systems is tailored

to meet the specific needs of user communities at all levels, by utilizing the systems specifically developed to meet their local needs, and is adaptable to change due to the loose coupling between systems.

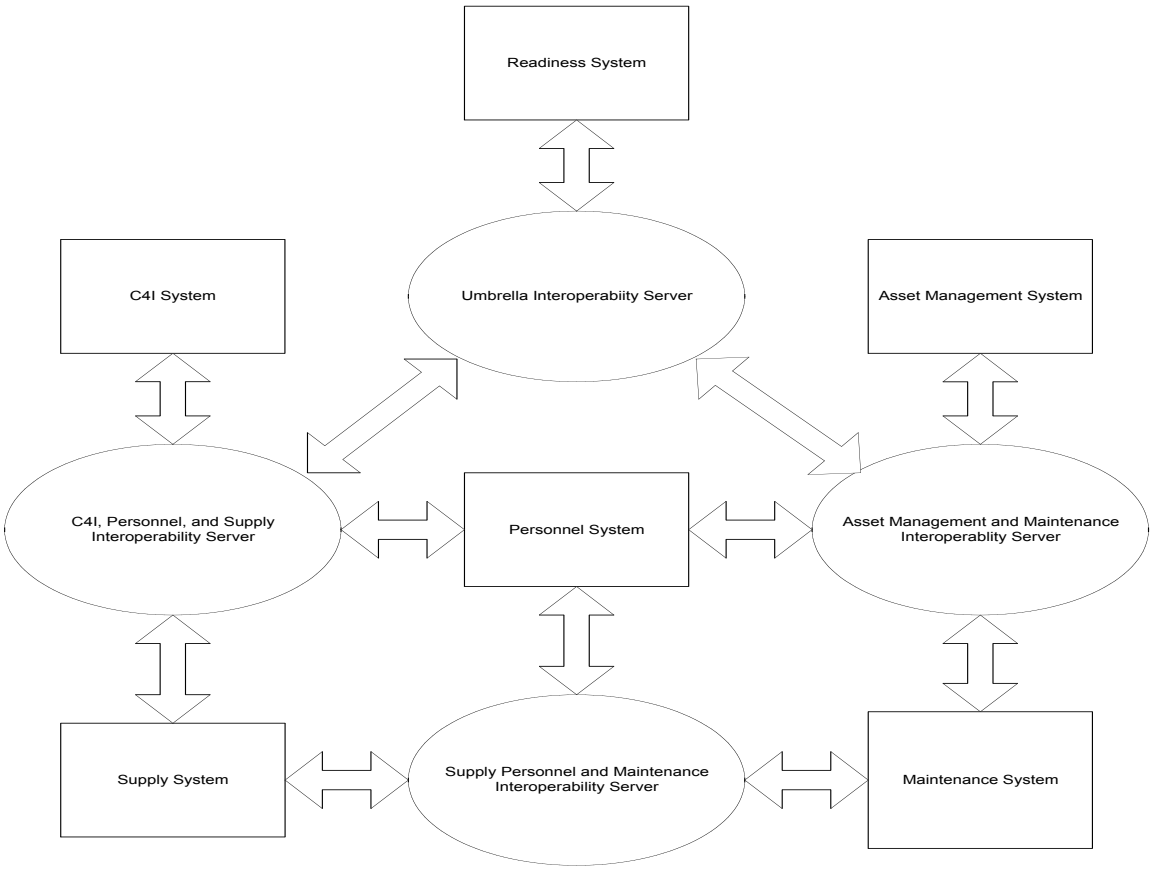


Figure 6: Interoperability Server

There will be several distinct ontologies associated with each Interoperability Server. System Interface Ontologies that are unique to each system participating in the federation will be used to define the interrelated logical constructs within the corresponding system that are targeted to participate in external interactions. For example, the System Interface Ontology for an air load planning system may include constructs to represent air transports, stow areas, and cargo items. Also associated with each participating system is an ontological map that defines the transformations required to translate information represented in the corresponding System Interface Ontology both to and from the Federation Interface Ontology. Federation Interface Ontologies that are unique to each federation will be used to define the interrelated logical constructs with which the client systems to the Interoperability Server may interact. This ontology defines all the information of common interest to the entire federation as opposed to the specialized interests of the individual systems that are participating in it. For example, the Federation Interface Ontology for a joint logistics transport federation, which interfaces specialized air, rail, and sea load planning systems may define a transport construct which is a generalization of the specialized air transport, rail transport, and sea transport constructs that may be defined by individual System Interface Ontologies of the participating systems. This ontology

once established serves as a standard for the domain represented by the federation similar in concept to the enterprise models that were popularized in the late eighties and early nineties such as the DOD Logical Data Model but exist within a more manageable scope and are driven by the interoperability requirements of the federation. Finally, an Interoperability Ontology shared by all Interoperability Servers will be used to define the interrelated logical constructs associated with interoperating systems and the services provided by the interoperability server. These constructs are independent of the logical domain entities associated with a specific federation. For example, the Interoperability Ontology may define constructs such as query, constraint, system, and ontology.

Summary

The key to the interoperability between systems lies with well-defined system and interface ontologies. An ontology makes explicit the conceptualizations used and shared by the interoperating systems. The shared conceptualization is known as the interface domain ontology. The interface domain ontology and the individual system domain ontologies should both be well marked up in terms of each other and ideally share both an upper level and lower level interface domain ontology. In this manner, the mappings that determine the context of interfaced entities on either side of the exchange are made explicit and are more likely to endure evolutionary changes to the systems and local modifications or special case usages. For systems to truly interoperate rather than just interface some sort of synchronization channel must be provided. As the number of systems participating in an interface grows even a well-designed information level interface can become unmanageable and an interoperability server approach should be considered.

The Development of Complex Adaptive Systems Based Decision Support Systems

John R. Hummel, John H. Christiansen,
Charles M. Macal, and Michael J. North
Decision and Information Sciences
Division
Argonne National Laboratory
9700 S. Cass Avenue/DIS-900
Argonne, IL 60439-4832

The submitted manuscript has been created by the University of Chicago as Operator of Argonne National Laboratory ("Argonne") under Contract No. W-31-109-ENG-38 with the U.S. Department of Energy. The U.S. Government retains for itself, and others acting on its behalf, a paid-up, non-exclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public and display publicly, by or on behalf of the Government.

Introduction

The field of complex adaptive systems (CAS) is providing a powerful approach to simulate complex and highly dynamic problems. In CAS applications, software "agents" can be created to perform the role taken on by the real-world players. As an example, the human immune system can be modeled using a CAS approach in which software agents are created to take on the role of antibodies. In another example, ecosystems can be represented as a CAS problem with agents representing the species in the ecosystems, specific individuals, or a more aggregated communal forms like "hive" or "flock". CAS applications can also be used to model economic markets with agents being created to play the role of producers, distributors, or consumers.

In this paper, we describe work being conducted at the Argonne National Laboratory to develop CAS-based decision support systems to address a number of critical problems. We shall give a high level overview of what CAS agents are and how they work. We will summarize a number of ongoing programs at Argonne that are utilizing CAS analyses and then give examples from two specific programs.

What is an Agent?

At the most fundamental level, an agent is a software representation of a decision-making unit. Figure 1 shows a simple example of a software agent.

A software agent is given a set of decision rules that describe the data and conditions (i.e., thresholds) that determine when and what kind of decisive actions should be taken. The conditions and courses of action taken can vary as a result of the overall environmental conditions and various measures of performance that can be applied by the agent, or the larger environment, to assess how "well" the decisions are being made.

It is common to see the phrase "intelligent agents" in discussions of various agent applications. The reality is that agents are not "intelligent" from the cognitive awareness perspective, but they can be made quite "clever" by the sophistication of the reasoning algorithms that make up their decision making processes. As an example, a pricing agent could adjust prices for a given commodity based on a predefined relationship between supply and demand. However, the relationship could be adjusted to give higher prices if it is determined that (1) the commodity in question is critical and (2) consumers would accept the higher prices because there are no alternatives available.

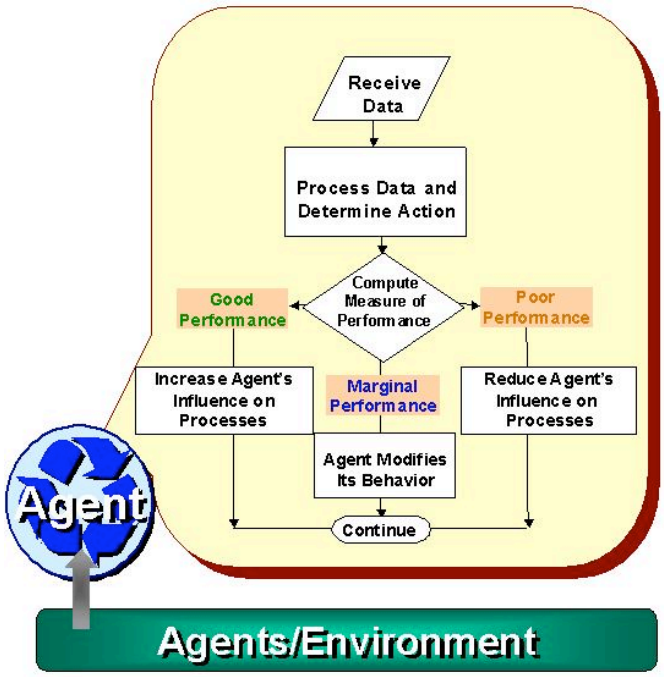


Figure 1. A schematic representation of how a generic agent can operate as a "decision-making" unit.

Agents are often characterized as being autonomous, semi-autonomous, or interacting with humans. Autonomous agents are those that can perform a given role without having a human in the loop. An example, could be an agent that automatically reorders stock items if the quantity on the shelf falls below a set level. A semi-autonomous agent is one that is given a set of conditions in which it can make decisions without human interaction, but is also given a range of conditions in which it must alert human operators and either inform them that the agent has performed a specified action or inform an operator of an impending condition that requires a human interaction and provides a recommended course of action. An example of the latter is the collision avoidance systems on modern aircraft that alerts the pilot that the plane is on a collision course and recommends an immediate course change.

In the military community, the majority of agent-based systems developed to support operators involve agents that interact with human operators as decision support tools that contribute to a course of action analysis. The agents can perform rapid analyses of complex situations and present one or more potential courses of action to take. But, the final decision will always be made by the human operator.

Complex Adaptive System Applications at Argonne

Argonne has a number of ongoing programs that involve the use of complex adaptive system simulations. These applications are addressing a number of problem domains, such as:

- **Electricity Markets** – The Electricity Market Complex Adaptive Systems (EMCAS) model is an agent–based model that simulates complex, realistic electric power markets.

- **Infrastructure Interdependencies** – CAS applications are being developed to study the interdependencies among natural gas, electric power, telecommunications, and petroleum networks.
- **Counter-drug Interdiction Strategy Analyses** – The Complex Adaptive System Countermeasures Analysis Dynamic Environment (CASCADE) program is being used to develop and analyze counter-drug strategies for interdicting drug trafficking.
- **Adaptive Communications Networks** – The Tactical Sensor and Ubiquitous Network Agent-Modeling Initiative (TSUNAMI) is addressing the U.S. Navy's shift from platform-centric to network-centric warfare.
- **Terrorism** – The NetBreaker program is studying how to identify hidden networks based on partial information.

In the remainder of this paper, we will provide some examples of how CAS is being used in the EMCAS and CASCADE programs.

EMCAS

The Electricity Market Complex Adaptive Systems (EMCAS) model is an agent-based electricity market model written in Java and using RePast*. EMCAS captures real-world behavioral patters, such as those observed in the California electricity markets. EMCAS includes detailed power marketing and transmission infrastructure markets, as represented in Figure 2.

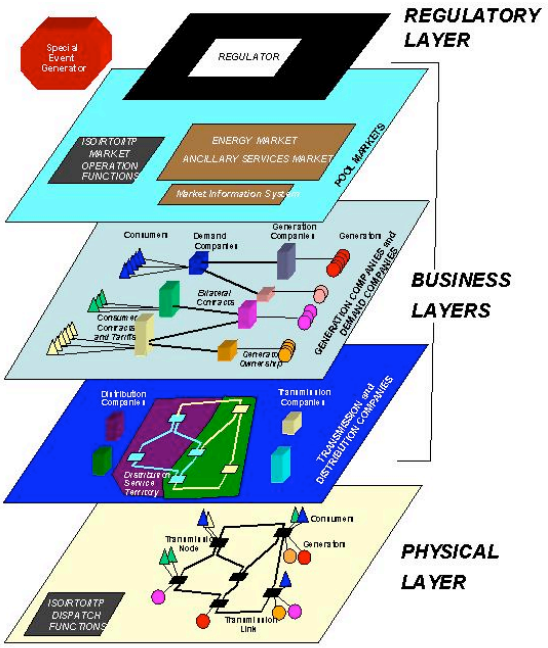


Figure 2. Schematic representation of the "layers" of functionality that can be represented in the Electricity Market Complex Adaptive Systems Model.

EMCAS agents take on the roles of individual market participants and are given the ability to make decisions based on various factors and different perspectives they can take on their part of

*Repast is a software framework developed by the University of Chicago's Social Science Research Computing for creating agent based simulations in Java. For more details, see http://repast.sourceforge.net/index.ph.

the market. For example, Figure 3 shows how an EMCAS generation company agent can look ahead and back in time as well as take a snapshot in time of the conditions facing it and competitors in order to make a decision.

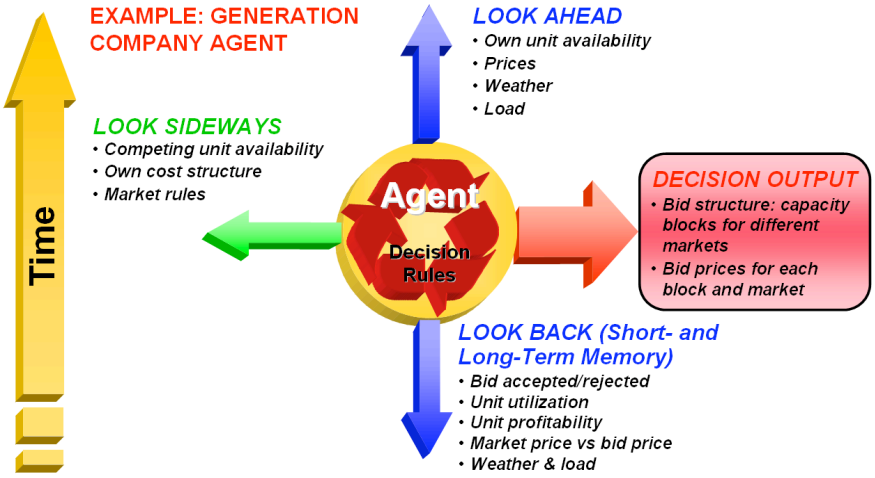


Figure 3. An example of how an EMCAS generation company agent can "look" in different temporal directions when making decisions.

All of the EMCAS agents work toward improving their own positions as they compete in various markets that are available to them, as represented in Figure 4. Individual generators and generation company agents can bid their generation capacity into any of the energy, bilateral, or ancillary services markets, subject to technical and physical constraints. Demand agents can satisfy their loads by bidding into the energy and bilateral markets. Demand agents cal also bid the curtailment of interruptible loads into the ancillary services market as non-spinning (generators not spinning) reserve.

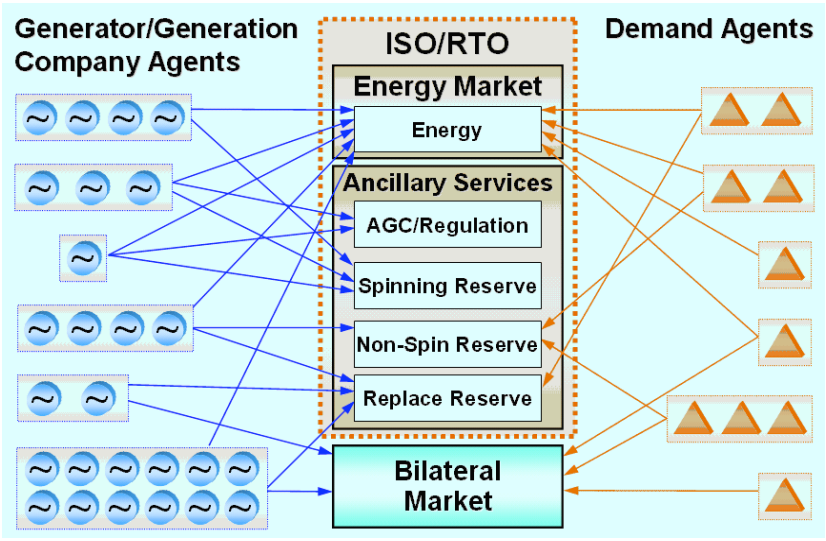
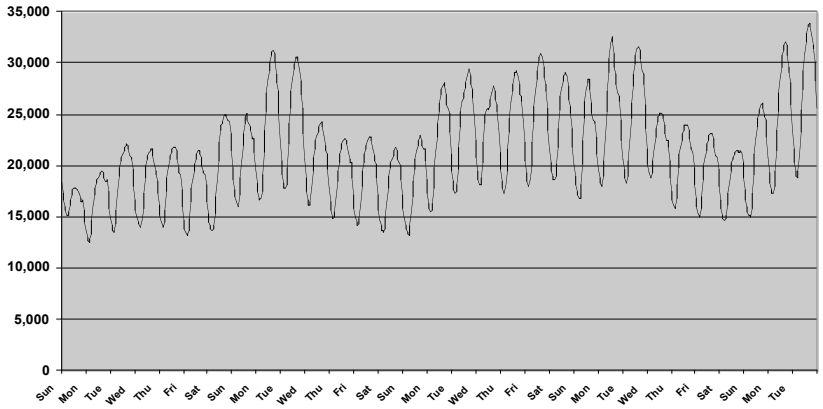


Figure 4. An example of how EMCAS agents can interact with different components of an energy market.

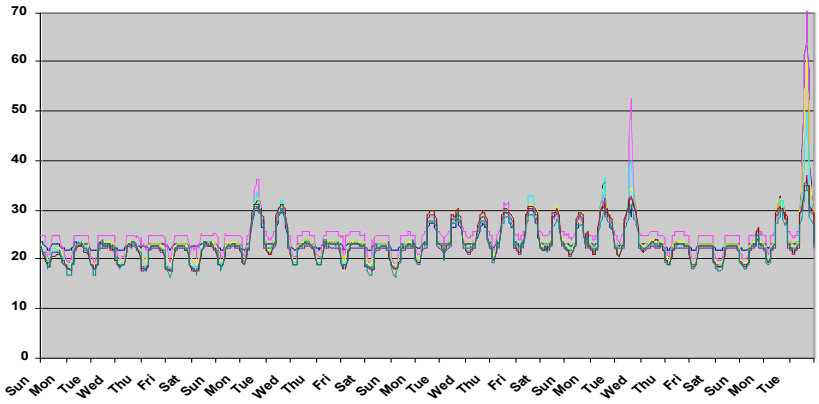
Finally, EMCAS agents can learn about their market and the forces that impact it, and make adjustments to their decision making processes. This is demonstrated in Figure 5, which shows (a.) the load served by a given market and (b.) the locational marginal price (LMP) in dollars per megawatt hour.

LMP is a tool for calculating the wholesale energy price for each location, or node, on a network grid. It can be used for scheduling power on a transmission system that recognizes potential transmission bottlenecks so that production schedules are consistent with real-time system limits. LMP is also used to allocate the use of limited transmission facilities to energy buyers and sellers in a non-discriminatory and efficient manner. Finally, LMP is used to make the best use of transmission and generation resources to serve loads and provide system reserves on a least-cost basis.

Typically, the LMP closely follows the load pattern. In the example shown in Figure 5, the LMPs increase at high load conditions. When a second and third peak in the load occurs, prices spike even higher as agents take advantage of the situation.



(a.) Load (MW) as a Function of Time



(b.) LMP ($/MW hour)

Figure 5. An example of results from an EMCAS simulation in which agents "learned" about how the market reacted to a power outage and responded when a subsequent outage occurred. (a.) The load as a function of time and (b.) the LMP as a function of time.

EMCAS is being used by the Illinois Commerce Commission to investigate the dangers posed by possible transmission constraints in Illinois in 2007. EMCAS agents are being used to simulate specific market participants, and the model will be used to determine the kinds and magnitudes of threats presented by possible transmission constraints.

CASCADE-CD

The Complex Adaptive System Countermeasures Analysis Dynamic Environment for Counter-Drug Applications (CASCADE-CD) was developed with support from the Joint Staff/J-8. CASCADE-CD was developed to aid drug analysts in deriving and justifying force structures and operational planning recommendations. It has also served as a "test bed" for the use of CAS techniques in "industrial strength" applications with the Department of Defense, such as developing new force structures and operational doctrines.

The focus within CASCADE-CD is on the drug "transit" zone for cocaine in the eastern Pacific, Caribbean, and Central America, with a limited representation of the "source" zone (e.g. Peru, Colombia, and Ecuador). The model explicitly represents the entire interdiction chain, including intelligence cueing, detection, sorting, monitoring, interception, visual identification, tracking, and the law enforcement "endgame." The actual geography of the region is considered as well as the attendant geographic and geopolitical constraints, such as the requirements to get overflight approvals from the various countries in the region. Finally, the drug trafficker "enterprise" activities are treated as being embedded in the South American socioeconomic matrix.

The scope of the problem addressed by CASCADE-CD is exemplified in Figure 6. The left panel shows the primary smuggling routes taken by the cocaine traffickers before 1995. The "Blue" force that was created to interdict these routes was optimized for air interdictions and assumed the "Red" (i.e., drug-trafficker) forces would remain static. Between 1995 and 1998 (see the right panel), however, the Red forces became frustrated and adapted their forces to be able to accommodate ground and river routes. The Red route changes involved relatively low cost and rendered the air-dominated Blue force structure less effective.

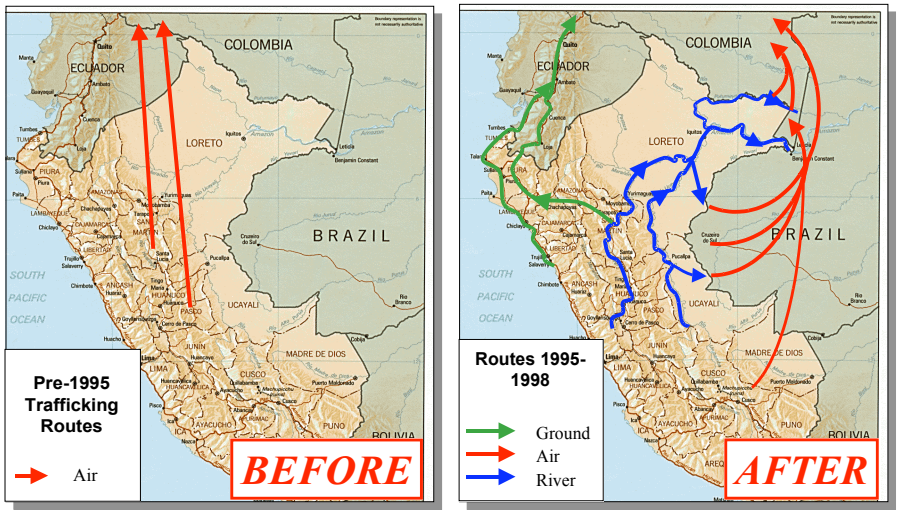


Figure 6. Historical scenario illustrating the scope of the problem being addressed by CASCADE-CD. Before 1995 (left panel), the Blue interdicting forces built a force structure in response to air-based drug trafficking routes. Between 1995 and 1998 (right panel), the Red trafficking forces adapted to the Blue force structure and began to favor ground and river routes.

On both the "Blue" and "Red" sides, adaptive behaviors are manifested in the agents at several scales and granularities, as represented in Figure 7. The figure shows different kinds of planning processes and steps that are taken by both the Blue and Red forces. The size of the different decision loops is meant to convey a feeling of where in the overall organizational structure a given process would occur. In some of the processes, an operations "stance" is created which is a set of dimensionless parameters that define an operations plan.

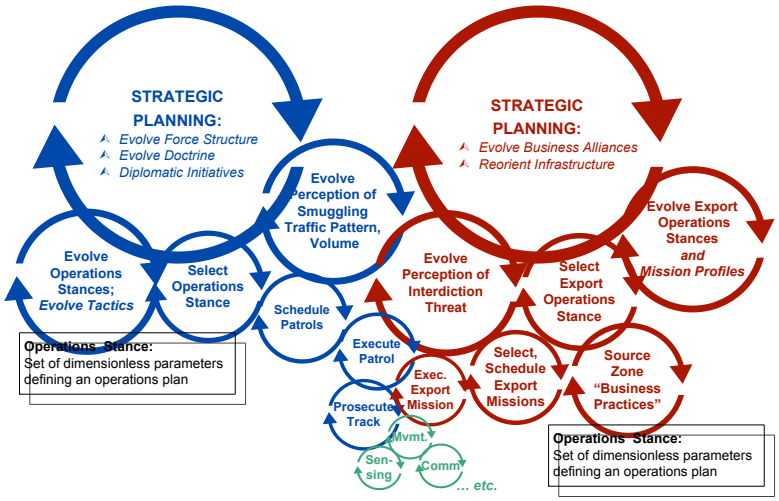


Figure 7. A representation of how the dynamic processes within CASCADE-CD are modeled at different scales and scope.

In developing the organizational structures for the Blue and Red forces, it was observed that while there is an organizational structure to the Red forces, it is not monolithic and hierarchical like that found in the Blue organization. Instead, the Red forces are an "ecology" of diverse organizations, like that notionally shown in Figure 8, and the modeled "cocaine trade" is the emergent behavior of "agents" working their own agendas.

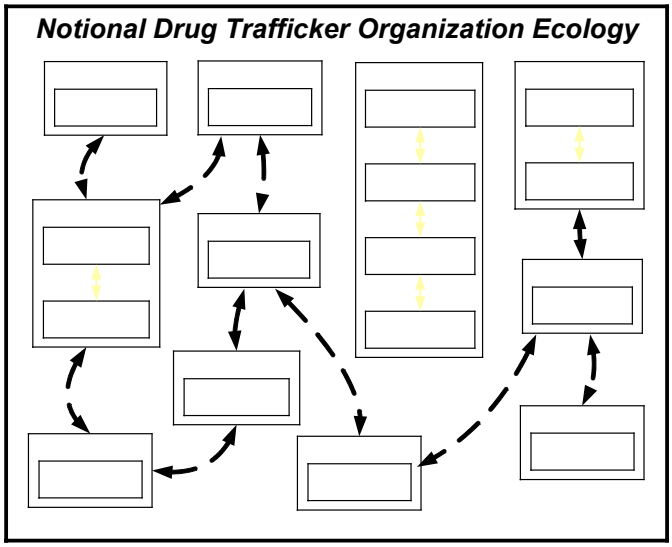


Figure 8. A notional drug trafficker organization ecology.

The counter drug operations that are performed are strongly asymmetric with respect to command, control, and communications in that the Blue forces tend to conduct theater operations under centralized control directed towards communications averse Red forces. In order to achieve success, an unusually high degree of coordination across diverse organizational boundaries (US military, participating nations, and law enforcement agencies) is required. This is especially true in dealing with air tracks, where timing is everything.

Genetic algorithms are used in CASCADE-CD to describe the behaviors of both the Blue and Red agents in terms of "operational stances" – a collection of parameters that address factors that are important to each side. Figure 9 describes the genetic algorithm factors used by the Blue and Red agents.

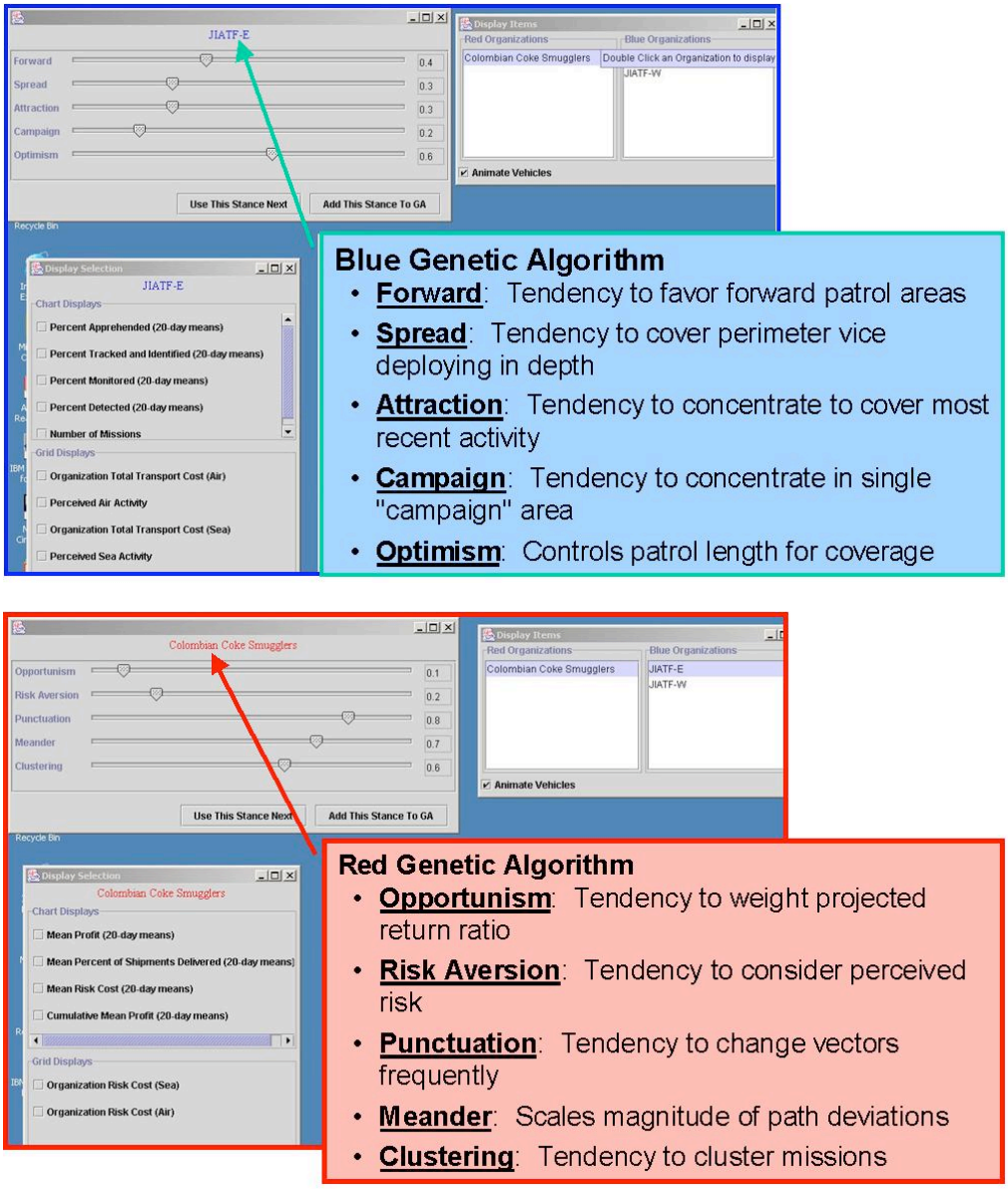


Figure 9. Description of the genetic algorithm factors used to describe the Blue force behaviors (upper panel) and the Red agent behaviors (lower panel).

During a simulation, a user can allow that agent's genetic algorithm to "evolve" better operational stances or the user can manually reset the value of each of the different factors using a simple slider bar. During a simulation, the behaviors of the agents change as they assess how well their plans are succeeding according to the behavioral conditions they have defined. For example, drug traffickers may vary their routes as they assess the "pros" and "cons" of the routes they are facing. A drug trafficker must weigh tradeoffs involved in selecting effective smuggling routes. A circuitous, meandering route to a destination is attractive to the smuggler in that it will make it harder for interdictor sensor systems, especially Doppler radar systems, to discriminate the flight from background air traffic, and will make continuous monitoring of the flight more difficult. On the other hand, the meandering route exposes the smuggler to interdiction for a longer period of time, and also requires more fuel than a beeline route to reach the same destination. CASCADE-CD explicitly models the sensitivity of a sensor system's performance to target aspect angle, radial velocity, and time since last vector change, so this rather subtle dynamic can be captured in the simulations.

CASCADE-CD provides a number of ways to review the results of a simulation. Figure 10 gives an example from an animation showing the interdiction of a P-3A EW aircraft maneuvering to monitor a drug trafficker flight. In this example, the drug trafficker's perceived air transport risk is shown as a color coded surface over the path being taken. In the example shown, the drug trafficker's organization believes the total transport costs over Costa Rica to be high due to its perceived significant risk of interdiction in a given area, and is therefore bypassing this area to the west.

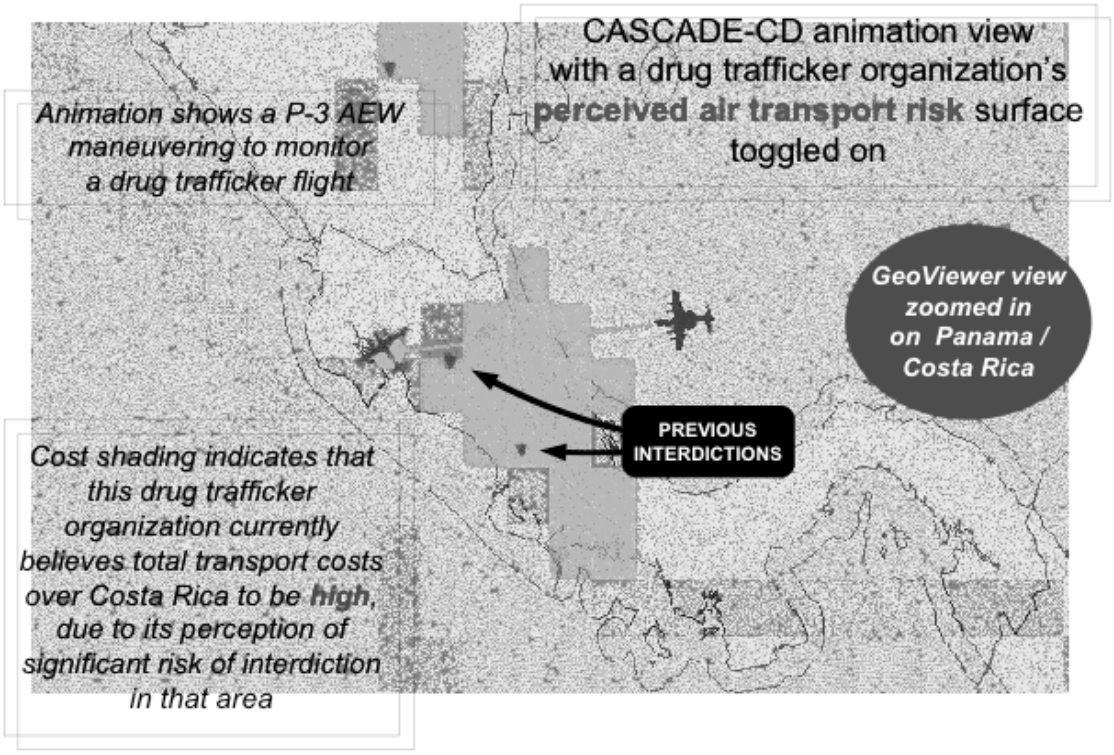


Figure 10. An example of a display from an animation view showing an interdiction between a Blue and Red asset.

Summary

The field of complex adaptive systems (CAS) is providing a powerful approach to simulate complex and highly dynamic problems. In CAS applications, software "agents" can be created to perform the role taken on by real-world players. Argonne National Laboratory has developed a number of CAS applications that are being used to study a variety of problems. In this paper, we gave an overview of these programs with specific examples of two programs.

Acknowledgment

This work is sponsored by the U.S. Department of Energy under contract W-31-109-ENG-38.

Information in the Execution of the Homeland Security Mission

Mike O'Neil
The Boeing Company

Introduction

The first thing I want to do this morning is say thank you to the Office of Naval Research and the Collaborative Agent Design Research Center for allowing Boeing the opportunity to talk here.

There are two important things I really want you to remember this morning, and they will be the central themes of this presentation. First, homeland security can only be solved by a government/commercial partnership, and second, many of the problems in the homeland security space can be solved today.

The domain of homeland security is not a problem that is going to be be solved by the US government alone. I am completely convinced, as many of you are in this room now, and even more will be by the time I have finished talking. This is a problem that is only going to be solved by a governmental and commercial partnership There are some very valid reasons for that. Sometimes when we get, what I call "window fixation", we don't understand completely. I hope by the time I have finished this morning you will have a much better understanding why a partnership is the way to go after the problem solution.

The second thing I want you to remember is this: many of the problems in the homeland security space can be solved today. These problems are solvable today because really where the challenge lies is taking a lot of what Secretary Lee talked about yesterday -- making data into actionable information and causing that to be distributed to the right decision-maker, and some of those decision-makers are machines. So those are the two major issues that I want to communicate to you today and I will probably hit them several times.

Figure 1: Agenda

First, we are going to do a little bit of what I call homeland security 101. We will define the problem space, look at imperatives to the solution, and talk about the current status. Then after we get done with what I call the classroom, we are going to say ok, that is great, you have done a great job of doing what everybody has been doing for the last two years, what can we do today? What is realizable today that doesn't require a large amount of energy? (as an interesting note, although I wasn't sure of all the other parties that were going to speak today, I think you will find that I am going to talk about this morning many of the things you are going to hear later on today), and finally, we are going to revisit why information is the essential tool for security of America's homeland.

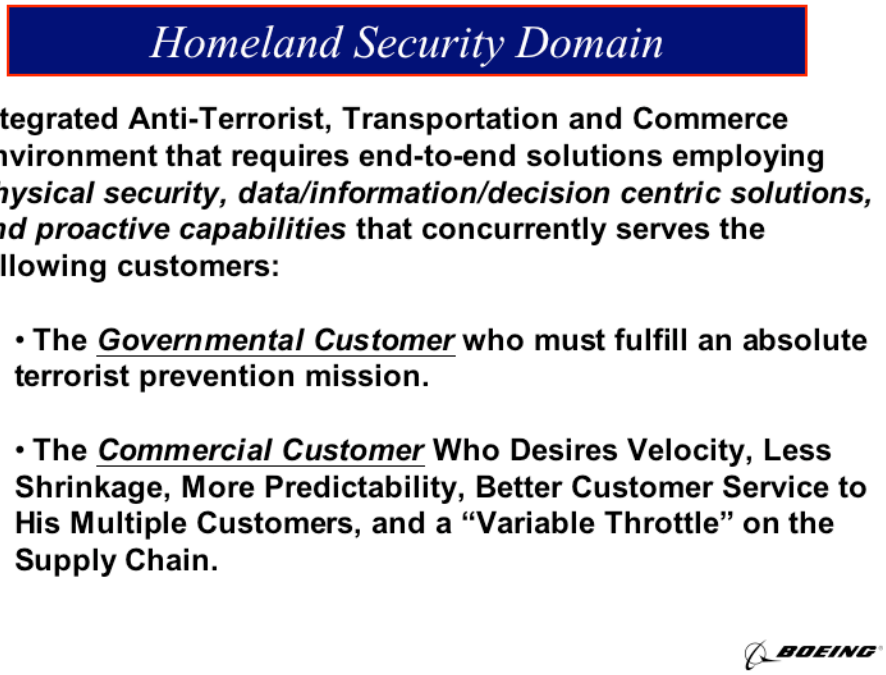


Figure 2: Homeland Security Domain

This is how the Boeing Company defines the homeland security domain (Figure 2). A couple of things are significantly different from how many people look at this. In America, we have focused an inordinate amount of energy on physical security. Here is what physical security is to homeland security. In military parlance, physical security gives you the current battle, it is the current operation, but you know what the problem is with that? You are only fighting the current operation and this guy who is your enemy, an asymmetric enemy, he is going to beat you about six out of seven days out of the week, so you have to figure out a way to get into the future operation using that same military parlance to homeland security. We believe the only way to get into future operation is through use of information. We start with data. Yesterday we heard some definitions of how does data become information. Our perspective is: data becomes information when it becomes decision relevant. If it is not decision relevant, it is not information. Why do we look at it that way? Because the speed of your operations, the speed of your decision cycles, and the momentum of things coming at you, if it is not decision relevant, it is really not important to be in front of a decision maker, so we take a little different perspective on that. Let me just be very clear: that is a perspective we see from the homeland security domain. We have done a significant amount of work in the area of network-centric warfare

through the Department of Defense. We are more in line with what Secretary Lee was talking about yesterday; but homeland security (if you use military parlance) is a proactive defense. Homeland defense, which is what is going on in Iraq right now, is a proactive offense, so homeland security is really a proactive defense approach.

Also, you have two customers you have to take care of all the time. The government customer is pretty simple. He has an absolute mandate to prevent a terrorist mission or a terrorist incident. Now, what about the commercial customer? Who are we talking about here? It took us a while to figure that out. Let me be very clear who the commercial customer is. The commercial customer is Walmart, Target, Costco -- the people who own the 100 largest supply chains in this country. They are the people who pay for the transportation and infrastructure that is commercially executed. Those are the people you have to offer value to. Those are the people who need to be partners in this. Why?

Let us talk about what happens if you have a terrorist incident, For example, let us say that there was an explosion in the Port of LA-Long Beach. There would be a small investigation. If it was determined that it was an unknown source, we would close down all the seaports in the country. Here is kind of what happens then. This nation runs on a manufacturing base that is driven by just-in-time inventory; the manufacturers have about two-and-a-half days of inventory on hand. If we close down those ports for over two-and-a-half days, and 95% of the raw materials comes through the ports on the Canadian or Mexican borders, you know what? We start closing factories. And, if we start closing factories, you take paychecks out of people's pockets and it becomes an immediate economic impact. So, we believe you need to be talking to that guy who owns that supply chain that drives that economic cycle, that is Walmart, Costco, Target, and oh, for some of you in the audience, the number 17 largest supply chain that comes into the United States is owned by Heineken, just in case you have an interest in that.

Figure 3: The Imperatives for the Homeland Security Solution

That is kind of our domain space. If you are going to solve some of these problems, what do you have to do? (Figure 3) First, you have to be transparent to commerce. If you are not transparent to commerce, you might as well be a card-carrying member of Al-Queda, because you slow down commerce, you slow down the speed of money, and as a result, you are doing exactly what Al-Queda does. We started with you having to be transparent, then we said that is not good enough, if you are going to talk to Target, if you are going to talk to Walmart, you have got to offer them value, or else they don't want to get on the train with you. You have to offer them an opportunity to increase their flow of commerce, you have to recognize, at the end of the day, this is simply asymmetric warfare. Sometimes we forget about that, because we get farther away from an unfortunate incident that happened two years ago. The bottom line is, you are fighting an asymmetric enemy, and as soon as you start forgetting that you are going to wander away from having an effective solution. This is something I think Rob Quartel will talk about a little longer, a phrase he came up with about two years ago now. You have to use time and distance to our advantage and push out those borders. What we want to do is find the problem in somebody else's country and stop it there. Instead of the enemy getting inside our domain, we get inside their domain, we have to have an ability to deal with it, but you know what, we are probably too late then. The key is finding this before it ever enters our borders. You have to avoid single point of failure solutions. Every day I get about four or five calls from people who have what I call silver bullet solutions that they would like Boeing to integrate into some of our products. You know what? There aren't any silver bullet solutions for this particular business problem and security problem, This is an broad problem, it is multifaceted, it is extremely complex and involves a lot of players. There is no single one thing you can do; so if you are going to try to apply a single point solution, you are destined to fail. You have probably forgotten about the asymmetric warfare facet because that asymmetric warrior, he is studying us, and he is using everything that is our weakness to his advantage. For example, he knows we are impatient, he knows we are time-sensitive, so he is going to study up, he is going to take advantage of that, so a single-point of failure is exactly what he is looking for.

Another thing, you have to be 100% interoperable. One of the biggest challenges of the Department of Homeland Security right now, is how to get 22 separate agencies all in a room, talking together, getting a common picture. We will talk a little later about how we get interoperable because, to be frank with you, it is part art, it is part science, and nobody's got the complete road map. We have some tools we think are helpful in that area.

You have to use data as a predictive tool. What do I mean there? You look at these asymmetric enemies, you analyze them, you analyze them both through governmental intelligence meetings, and a commercial means, particularly their financial fingerprints. What you are going to find is increasingly they leave what we call data breadcrumbs around the globe. We believe these data breadcrumbs from the asymmetric enemy need to be vacuumed up and used as predictive fuel. There are clearly methods to do that, and numerous different things that we'll talk about a little later,

Finally, it is global in nature. If you are thinking homeland security is only something you do in the United States, well, you are mistaken. Why? The United States lives in a global economy, the economy is what the asymmetric enemy is targeting, so if you want to just protect the United States you have probably forgotten part of your battle area.

Figure 4: The Imperatives for the Homeland Security Solution

You have to have customer buy-in. I spend a lot of time visiting large supply chain owners. Let me be very clear to you what they tell me. Have you talked to those guys in Washington and the government recently? We are really scared they are going to make some draconian rules and I won't be able to continue to sell T-shirts for $2.59 at Walmart. This is not a single one guy makes the rules, you have to have some consensus. I know I am not a guy who really likes consensus because it takes time. In this situation I am completely convinced it is the only way to do business. We have to avoid manpower intensive solutions. How many of you flew to this conference? You had an opportunity to visit a Transportation Security Administration screener, that is a manpower source that we had a really fast reaction to as a nation. We over-subscribed our manpower base, and it became a manpower intensive solution. We need to avoid that in these other areas where we can take a deliberate, methodical approach. If we don't there are a couple things that could happen. One, we are going to run out of money to really solve the problem and two, the more people you put in processes, the larger your potential for failure is. That is empirically proven over time all the time. So you are just going to assist yourself in having a problem later on.

Let us talk about forensics. Let us say that you have that huge explosion in LA-Long Beach, and the national decision is to close down all the ports. That is not how we need to do business; we need to be smarter than that as a nation. We need to have the ability to isolate where that problem came from and then look across the entire domain space and maritime commerce and identify any other commerce coming in, any other containers coming in, with the same attributes related to the explosion. Those get stopped. Let us turn everything else on, we need to be able to deliver forensics to the government. They are looking for it. They see it as a tool they can use to preclude a draconian decision after an incident. They also see it as its critical thing to assist in recovery after an incident, in the restart process. I think this goes without saying we need to stay dynamically ahead of an asymmetric enemy and close the seams.

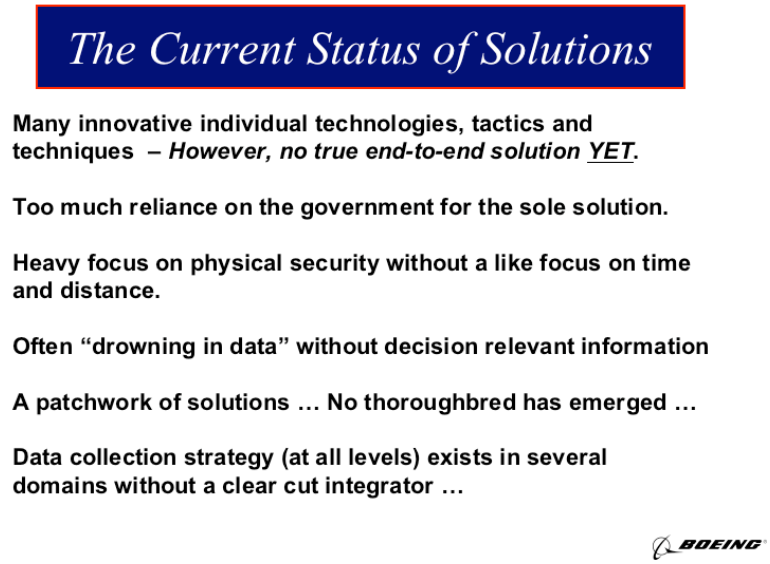


Figure 5: The Current Status of Solutions

Where are we at today? There is a lot of really innovative technology, tactics and techniques, but to be frank with you, I don't think there are any real end-to-end solutions yet. I think there are some folks who are doing some demonstrations. I think there are some folks with some good intentions, but is there a standard or a series of standards we could use throughout homeland security? No, probably not, because remember one of the things I talked about in the beginning? Information? We have not done enough to harness the available data and information to allow us to do this in an efficient and effective manner. We may be able to do it in an effective manner now, but we probably cannot afford it from an efficiency perspective,

I would like to use a little quote from Representative Rohrbacher from California. I was at a conference not long ago in Long Beach, and most of the folks in the audience were from either the California government or municipal governments or local governments, and Representative Rohrbacher said this (oh and I must tell you he was in shorts and a surfer shirt): "I must say, I am very happy to see you. A lot of you in the audience think the solution to homeland security is a large armored truck driving up to your office filled with government money. I am here to tell you that you are mistaken. You need to become part of the solution, because that is not going to happen." He embodies what I am talking about right there. If you think this is completely a governmental solution, you are wrong. It is not going to happen for three reasons: (1) they can't afford it, (2) they recognize the need for partnership to commercial industry, and (3) the problem is too big for any one entity in society to solve, it is that simple. So we have to help them find some outside focus.

Physical security, too much focus on physical security. In the area of port security grants there has been well in excess of somewhere around $5 billion that is gone out the door. If you look at it on a percentage basis, less than 10% of that money has been focused on technology solutions. The remainder of it has basically been into stuff that either does an assessment of physical security, or it buys closed-circuit TVs, fences and gates. That is an important thing, but fences, gates and closed-circuit TVs were a responsibility of the port long before we ever had a national awakening on the 11th of September. If you look at the potential of Al-Queda, attacking the port

of New York-New Jersey through a physical attack that would be stopped by a fence, is probably not going to happen. Those aren't Mike O'Neal's words. Those words are from the Director of Security at the port of New York-New Jersey who I talked to a couple of weeks ago. We have had too much physical security. Why have we done this,? To be frank with you, because it feels good and looks good on the national news. Is it where the ultimate solution lies? Probably not. I want to talk about that some more today.

Right here, we are drowning in data. Yesterday we heard about the challenges in DoD, the challenges in DoD, to be frank with you, are minute compared to the challenges in this domain. Why? Because it has traditionally been a commercial domain, there are loads of data out there, and on the governmental side, most of the data resides in stove pipes, so you either die in this commercial data or you can't get a hold of this other data, and the short answer is, it is very difficult to get to decision relevancy at the individual decision-maker level. What we have are patchwork solutions. We don't have anybody who is a collector and an integrator who has received national credentialing. There is a real need for that.

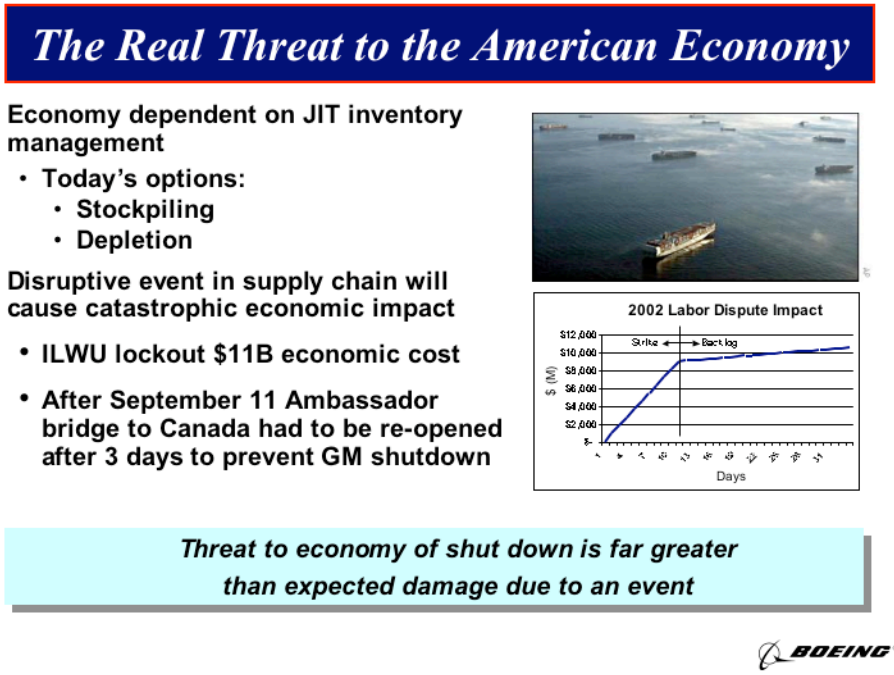


Figure 6: The Real Threat to the American Economy

We have some longshoreman unions on the West Coast. They caused a 10-day shutdown of all the ports on the West Coast. We were able to identify through dealing with the Port of LA-Long Beach a cost to the US economy based on the entire West Coast. They could document $11 billion, I think others of you have seen estimates of up to $20 billion, so you know, the short answer is anywhere between $11 and $20 billion. In my book you are talking real money. That was 10 days and that was just the West Coast. Most of the shippers were pretty smart and they started going through Canada and Mexico. Imagine if you shut down all the ports in our country, you would have a monumental influence. After the 11th of September, in order to keep the General Motors plants running in Michigan, the Ambassador bridge between the US and Canada needed to be reopened after three days.

The short answer is this, you might think homeland security is about physical security. It is about the economy. You have a governmental contributor, and you have a commercial customer contributor, and unless you do it that way, you are going to have a solution that doesn't work in the long run.

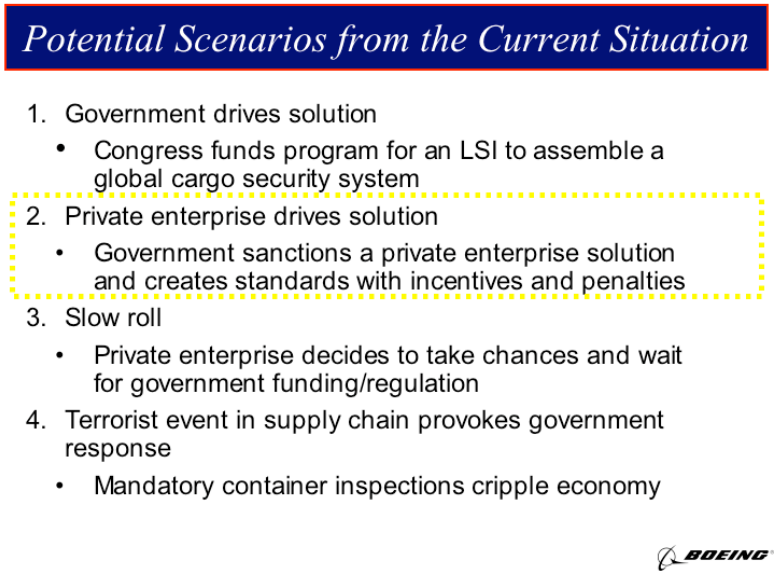


Figure 7: Potential Scenarios from the Current Situation

So what can come out of this environment? We can see the government driving its solution, and Congress funds a program, a Large Systems Integrator to assemble a global cargo security system. At Boeing, we thought that was what the road ahead was, because one of the things we like to do is to be large systems integrators. That is one of our basic core competencies. After about six months of looking at this problem we said, you know, we are fairly stupid, that is not going to probably happen, why? Because the problem is too big for one guy to take on.

The next thing, well maybe private enterprise drives the solution, we will come back to that in a second.

Number three, the slow roll. That is kind of really where we are at right now. If you look at the commercial enterprises, most of them are kind of sitting back waiting to see what comes out. They do not want to jump in with two feet, and they are waiting to see what the government will do. There is a little bit of communication going on, but it is really not a large amount of communication. Let us say an incident does occur, and we go to perhaps 100% container inspections after a period of shutdown. You know what? Osama is popping the cork on his champagne then because he has gotten everything he wanted, for maybe doing something that did not cost much.

What do we think the future holds? Private enterprise drives the solution. Government sanctions a private enterprise solution and creates standards with incentives and penalties. You have to have a commercial governmental solution set, if you do not, you are not going to solve the problem. You are either going to contribute to what the terrorist is looking for because you have

slowed the speed of commerce, or, you will have done something that prevents the government from fulfilling their absolute mandate of preventing a terrorist incident.

Realizable Approaches to a Better Homeland Security Solution

Now we have defined the problem. Next I want to talk about some things that have been done lately, very realizable solutions.

Boeing has an innate interest in air passengers, but we also have a very large amount of interest in cargo. Why? The area we still have to do a lot of work in is cargo. We decided rather than looking at this as a big defense company, let us look at it through a customer's eyes. When you talk to a customer about cargo, he basically uses a quadrant model. This quadrant model categorizes things either by value of loss, or probability of loss. When you look at it this way, it becomes very apparent that one size does not fit all. One example of high-value high-loss might be a 20-foot container of Viagra. A 20-foot container of Viagra has a retail market value of in excess of $10 million. It has a street market value of somewhere between $6.5 and $7 million depending on the domain you sell it in. Most of that Viagra is manufactured either in Puerto Rico or in other parts of the Caribbean. It is a high-value target that is frequently sought by people who steal things. So when you talk to Kaiser, they are interested in an absolute way to protect this because there is a huge amount of commerce and revenue flow. They need a solution that is very absolute, because there is a high probability of loss, and there is a high value to somebody stealing it.

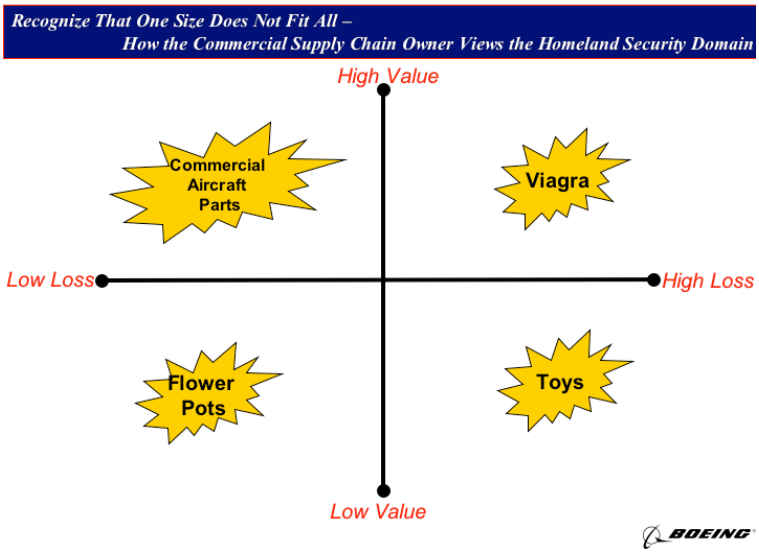


Figure 8: One Size Does Not Fit All

Commercial aircraft parts, something I am familiar with. We have a supply chain in the Boeing Company that originates in England, goes through every mode of transportation except air transportation, and ends up in Everett, Washington. It is been in operation for 35 years, there are zero recorded instances of theft there, you know why? Nobody steals 747 wings, there is no market for it. That is kind of unusual and we do not normally ship small parts, we ship

assembled parts because we bring them in and we put them together on a plane. We have a lot of things that actually fall into this high-value, low-loss category. What are those things of interest for? Commercially, all we really want to do is have in-transit value on that shipment so they can synchronize it to their manufacturing process. You know what this kind is perfect for though? If you are smuggling, it is a great place to put contraband. Now the government has a bigger interest in that and they need a little better view of it.

High-loss, low-value. I live out in California and that is the Mattel company right there, that is Barbie dolls. They are not that expensive, a container of Barbie dolls might bring you $800-900K depending on how they are packaged in the retail market, but boy those things like to get stolen! The other thing is, some of those high-loss, low-value items again offer great potential for contraband, because people don't inspect them.

There is a company located in the Philippines called Laura's Gifts. Laura's Gifts was one of the principal flower pot manufacturers for Walmart, Target and Costco. Flower pots are probably not something people in here commonly think about. I've talked to Walmart, I have talked to Costco, I've talked to Target, they are willing in a shipment of 100 containers to lose 3 of these containers. It does not bother them at all. You know who is really interested in these containers though? US Customs, because flower pots are ideal for smuggling, because nobody inspects them, they have cavities in them, you can put all kinds of neat stuff in. My purpose in showing you this is to show the intersection of the governmental customer with the commercial customer. The first time I looked at this it certainly opened my eyes and I hope that I have been able to communicate that to you today.

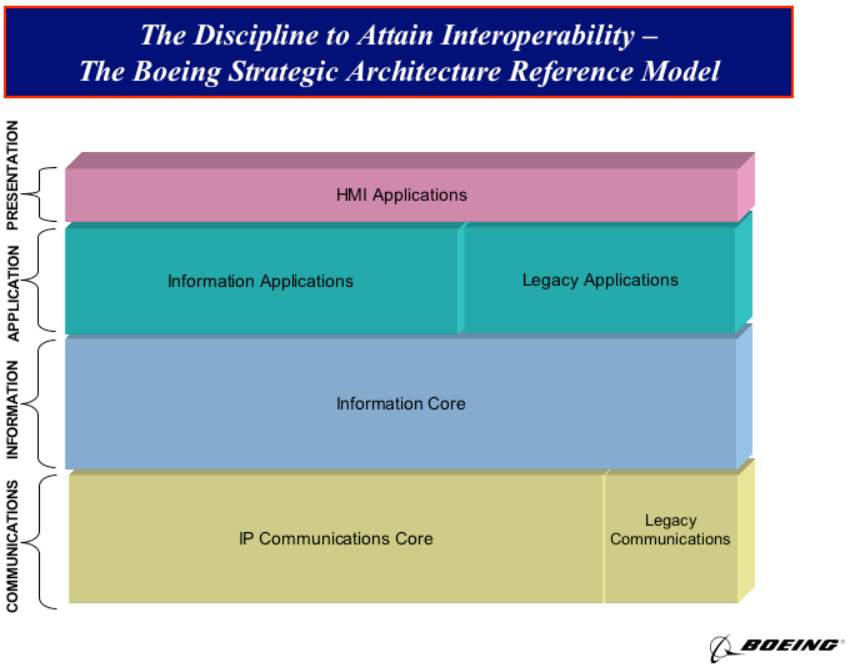


Figure 9: The Boeing Strategic Architecture Reference Model

How do we get to interoperability? Like I said before, it is part art, it is part science, and it is a lot of hard work. Within Boeing, what we use is this particular model here, which I refer to as

the brick, but some people a lot smarter than I have called it the Boeing Strategic Architecture Reference Model. What we have done is to take the essence of network-centric warfare and put it into a systems architecture approach. We use this model and every system we put out must go through this discipline, and it takes about 25% of our total effort for putting out a system. Why is this important? Behind each one of those blocks you can drill down through probably 100 other sets of rules, decisions, and you have to pass all those in order for us to solve the challenge of interoperability, we are going to use this for both of our operations-safe commerce demonstrations, why? We've told the customer we are going to be interoperable, this is the discipline we are going to apply to make that. Some of this is very easy to do, some of it is very challenging.

Human Machine Interface (HMI) applications.

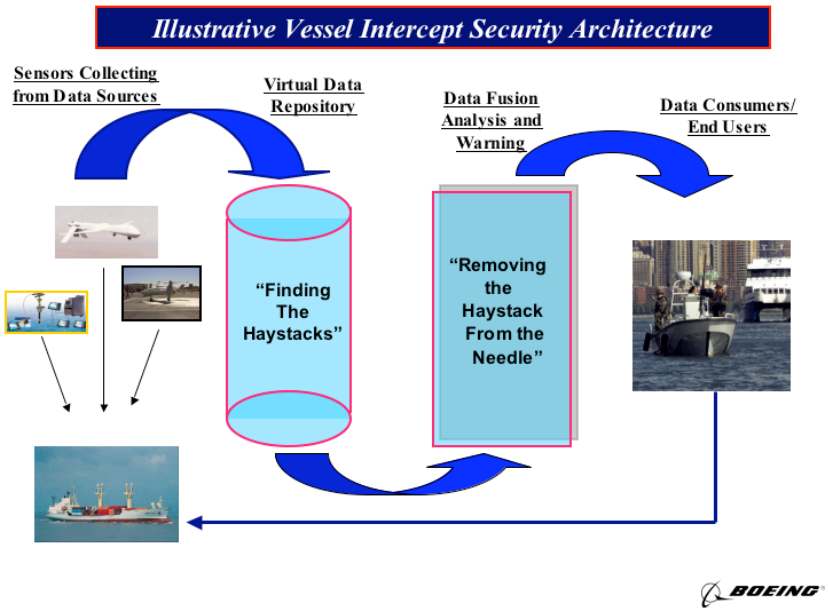


Figure 10: Illustrative Vessel Intercept Security Architecture

I want to talk to you about some things the US Government is doing, and some things that can be readily done to help improve interoperability. What you see here is an architecture of exactly what the US Coast Guard is doing to find bad vessels. There is a series of sensors out there. Let us talk about sensors for a second. Yesterday there was a lengthy discussion on sensors, I think we need, in the homeland security domain, to look at that word sensor and change how we view it, and how we define it in our minds. Most people think of sensors as maybe little round things, or maybe something that is on an unmanned aerial vehicle (UAV). That is too small a definition of sensor. We need to think of sensor as anything and everything that collects data. A sensor might be one of those little round things, but you know what a sensor could be? It could be an entire airport system, it could be an entire seaport system. The way you need to think of it conceptually is anything that collects data that ultimately becomes decision relevant. If you don't think about it in that way in the homeland security realm, you remember about the asymmetric enemy? He is going to take advantage of that, because what he is trying to do is find some seam in you decision-making and get in between that seam to get his mission accomplished. I wanted to say this about sensors because I noticed that discussion yesterday and

most of the sensors in DoD are either focused on targeting processes or defensive processes, and the homeland security environment. Because you are serving two customers that are significantly different, the way you view and use sensors is perhaps a little different.

They are collecting information here, and some other intelligence. You want to find the haystacks, the virtual data repository. There are several of those, the Coast Guard has a large virtual data repository, dealing with vessel tracking. There are also some Navy and Coast Guard operations up in Suitland, Maryland that do the same thing. We are going through here, and they are finding these haystacks, then they go through some fusion analysis where they remove the haystack from the needle, and then they go back to their consumer which is one of their security patrols in a harbor, and they are going to do some type of interceptive boarding process, this is all done today. A year ago today there was, a major event going on in New York City, and offshore there was a vessel that had alerted three times for radioactive materials. There is a reasonable degree of national concern about this, why? The president was in New York City that day. An interagency boarding party, Coast Guard, Customs, DOE went on board that ship. They did a series of checks and here is what the short answer was: it absolutely had radiological material on there, it was the red paint on the plates that were inside the vessel. Why do I use that as an example here? This will find that vessel, what this doesn't do is remove the false alarms and the nuisance alarms in the process, is that information available? Yes, it was, it was available through commercial data systems. The problem is this particular process uses very little commercial data, in order to target their thing. That commercial data is available today, it can be gotten from commercial providers, protected in a firewall environment where their intellectual property is protected and it would solve some of that resource application. If you go talk to Governor Ridge, his biggest problem is applying resources across his entire spectrum of problems. What I am trying to do here is demonstrate bringing commercial data into this decision cycle, you would be able to figure out what the problem using the business process cycle vice before it became a national level of concern.

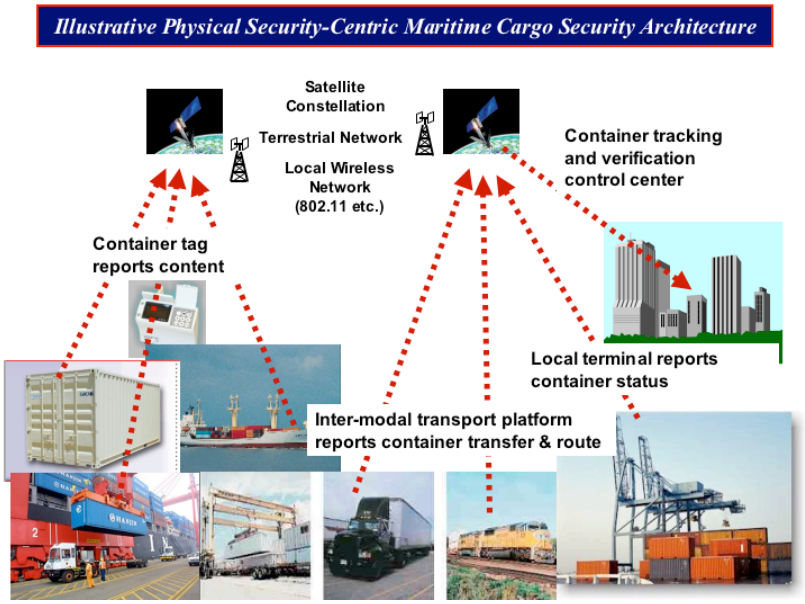


Figure 11: Maritime Cargo Security Architecture

We are going to do a couple of demonstrations for the Transportation Security Administration. We are basically going to do end-to-end instrumentation of a supply chain. What we are going to do is one supply chain starting with flower pots in the Philippines. We are going to go to the factory where they make those flower pots, and we are going to put in closed-circuit TV cameras. We are not going to have a person watch those cameras all the time because people fall asleep, they have to go to the doctor, or sometimes they have bad days. We are going to take those closed-circuit TV cameras and put intelligent agent decision alerts into them, so when things that happen in the process that are not supposed to happen occur, they notify a human being. For example, part of the process at this factory is stuffing the flower pots inside a container. The outside of the flower pot contains a radio frequency identification tag. If somebody puts a flower pot inside a container that doesn't have a RFID tag on it, the agent causes an alert that causes the system operator to go in there. Why? Because if it didn't have an RFID tag on it, it is not supposed to be in that container because it is not certifiable cargo. That is a small example; there are about 75 of these different decision rules that agents check for. So we are going to start there, we are going to make sure everything that goes inside the container is free of the capability of a terrorist to use for something that he'd like to use it for. Once we get the container stuffed, we put what I call a little smart box inside the container. A little smart box will do two things, one, it will detect breach of that container anywhere in the material surfaces of the container whether that is a door opening, somebody drilling a hole in it, so on and so forth, and two, it will give us an autonomous position location of that container as it goes throughout the transportation length, so we have an immediate ability to have in-transit visibility and we also can tell if somebody wants to get inside the container. We seal it up and we write that off, then we start transmitting that information back, now here is kind of the interesting thing, as you all know, the government's bought a couple of things from Boeing over the years. They've bought a couple of large network operation centers, and the government has enough excess capacity in some of those network operation centers to allow us to use that capacity to service a Transportation Security Administration to see this in-transit visibility in this whole process. There is some capacity both in terms of network and presentation layer that we are going to use to allow the government to see this, why? Because they have already got it, it is theirs. Once this thing goes on a wheeled vehicle from the factory to the port of embarkation, we have a whole separate subsystem that tracks the wheeled vehicle and reports into this same presentation layer. Interestingly enough, remember, this information is being collected in the Philippines, the network operations center is over in Leesville, Virginia. We are doing this through use of satellite communications which again is another thing the government has purchased through Boeing so we are leveraging some additional capacity that is available there that they've already bought. Why are we able to do that? At the interagency level, we see this capacity, so we talk to the one customer over here who maybe bought the satellites and say, is it ok for this other agency to use it, and generally they are going to say, sure.

You get into the port and at the port we are going to do one other thing. It is going to go through a radiological nuclear detection system, because that is a large possibility of a problem. This whole process gets repeated throughout the entire cycle, where this container gets off-loaded in LA-Long Beach. Then it is going to get on a wheeled vehicle and moved to Carson, California. That is where the container gets unloaded. We will be notified back in Leasburg that they are getting ready to unload this container. We will de-activate the smart box so we don't get false

alarms, then we open up the container and unload it. That is what we are going to do in our two demonstrations. We think that is really interesting, but one of our senior managers said, you know, that is interesting, but that is not good enough. All you are fighting is the current battle, you never see into the future. What we have done, is wrapped a risk assessment engine around this whole product, so we have this physical security-centric layer that fights the current battle, and you have the risk assessment engine that fights the future battle. Both of those feed into our database that provides decisions at different points in the process, you have to do physical and data layer.

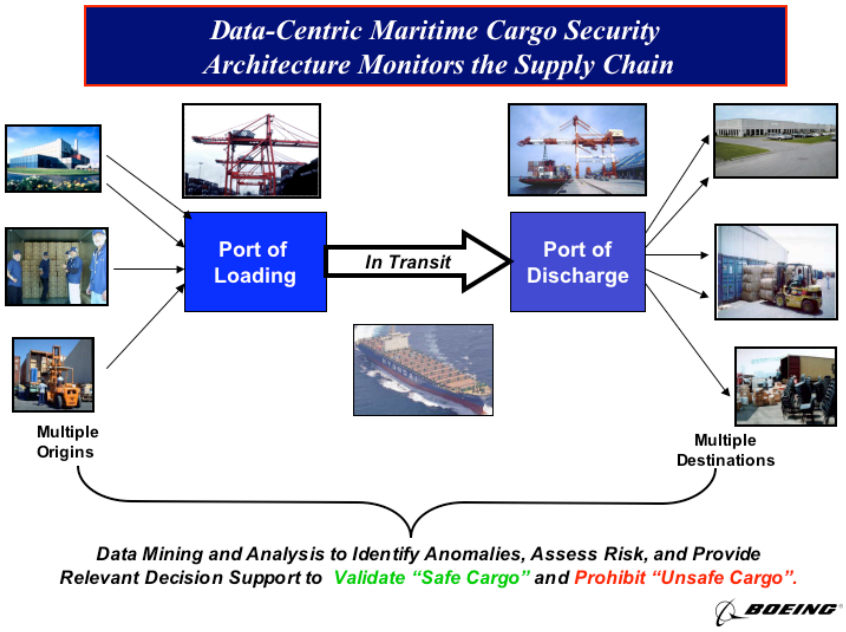


Figure 12: Monitoring the Supply Chain

Here is a good example of what we are going to do with our risk assessment engine. We are going to do some pretty serious data mining and analysis. Getting the data is the hardest part of doing this. Why can't we get the data? We've entered into a partnership with an unnamed company that owns one of the largest supply chains in America, the first time I visited them I was amazed. They had 54 people there that worked in security and risk assessment on their supply chains. That is a lot of people, and they said, we would like to work with you all, but you can't tell anybody who we are except, you know, the government. We would like to work a lot with you on figuring out how to get a really advanced risk assessment tool, we said, oh, where have you been, would you like to go out to dinner tonight, you know, please, and we are going to do that, so that will provide us an opportunity to get that data, now what did they want from us? They said, we want no release of our intellectual property and we said, we understand that, we have the same problems all the time, let us show you how we've fired all that stuff off for different applications and they said, for this demonstration, you don't have to use government classified data, but if you want to do work with us in the long run, you have to be able to do that, so we are dealing with part of the challenge here is how do you make the transition between all the different modes, because when you go down and talk to the Noel Cunningham or Bill Ellis at the Port of LA-Long Beach, they don't want government classified data because they cannot deal with it in their domain, what they need is the decision relevant part from that data, for example,

stop container 1234 because it contains a threat. They do not need to know the reason it contains threat is we did a financial forensic analysis on it and most of that money came out of a small bank in Pakistan that is directly related to Al-Queda, they don't need to know all that, they just need to know, so you have to do some filtering things.

This is not a complete art, it is not a complete science, it is a developing area, it is the largest single place where you can make progress to date in my estimation homeland security, why? The asymmetric enemy is using all of our weaknesses as his strength, this is a way that we can reverse that equation, and to me, this is where you make the money.

Let us talk about a couple of things we have found out in looking at this whole domain space. I apologize for having such a simplistic approach to this, but for me it made it very easy to understand.

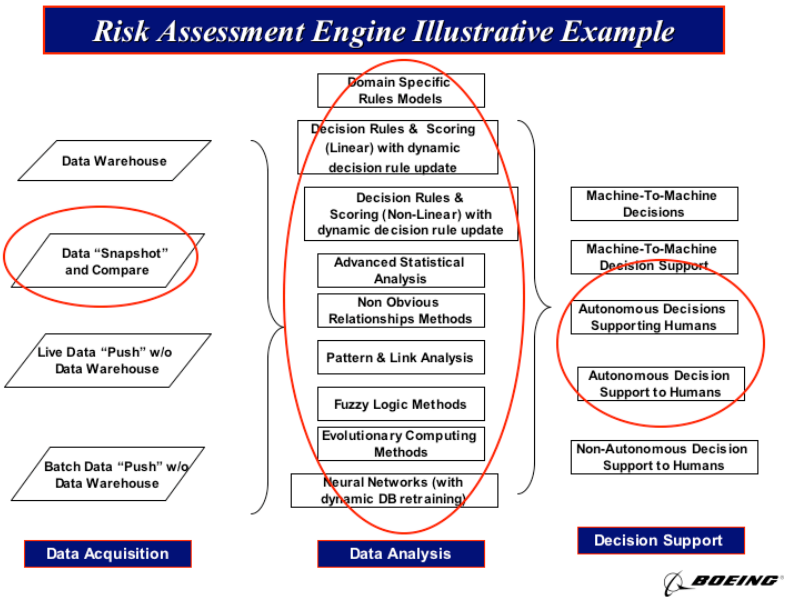


Figure 12: Risk Assessment Engine

Here is the first thing we found out when we started working in this domain space, that it made a lot of sense to build a data warehouse. People don't like to build data warehouses in the commercial world because then they are giving up their intellectual property, and they worry about what happens to that because of competitive disadvantages. We found someone who said, you don't need to build a data warehouse. We will make an intelligent agent. This agent will use decision rules to examine the records in databases, and make a binary decision. After this binary decision is made the agent goes back to the decision table and records it. Here is a big competitive advantage in using this particular approach. First, if you think back to my quadrant for types of cargo, that flowerpot guy does not need an advanced non-linear equation in all likelihood to solve his problem. He probably just needs some simple decision rules. The guy selling Viagra, he is going to pay for the most advanced capability he can get because that is $10 million of revenue that is gone if that container is gone. We need to look at that commercial customer and see what he is looking for. Then look at the governmental customer, he kind of fits in a quadrant too, because the likelihood of terrorist incidents occurring or being originated in

certain countries is much lower than in other countries. For example, we were originally going to do a supply chain that originates in Pakistan, because we thought that was a pretty hard one to do. We ran into two problems, the government (TSA) was concerned that if something goes wrong, and someone get injured, there is a liability issue there. The commercial guy, he was still on board with us, but then we went back he did a demand forecast, most of the companies he was buying stuff from that go through Pakistan are no longer in business. There is a much lower likelihood of something going wrong in Felixstowe, England. So you use the same approach in looking at what type of perhaps risk assessment. Now is there a straight line of decision rules in use? No, no there isn't, you have to learn and you have to use these same tools to help you figure out what rules to use.

What we think the domain space needs to focus on after decision support is autonomous decision support and humans. This is a tough one, what I am talking about there is machine to machine stuff that occurs that human beings don't even know about. In the area of commerce and transportation, there are loads of those things that can occur. Now the problem you run into is across both of these customer bases, governmental and commercial, there is a natural resistance to machine to machine communication. You have to educate them. Let me give you a good example of something that is completely logical. Let us say you are screening air cargo, and your radiological devices, you have a double positive check before they pop positive, if both of those things pop, you know what, you might as well just ground that container because it does need to be physically inspected. Then, by notifying a human being that some other process, you might as well just put it aside and have it inspected, why? Because the likelihood if you got through a double positive check is very high that something's wrong there. The other thing is, autonomous decision support, two humans, it is a nice word, it is a nice bumper sticker word, what are we talking about? A guy gets notified that he needs to do something , and he has to having to read volumes of books, it is easier to be notify the what, the where, and the why to the support security director in LA-Long Beach, he needs to have a PDA and he needs to get a little alert on it, ok, maybe one of his guys who runs his harbor patrol gets an alert under the dash inside the patrol car, maybe back at the regional TSA center there is just information that comes in, but everybody's got a little different part of the decision, some of them are informational, some of them are action, but they don't need to know necessarily everything, the reason they don't need to know everything is because they were doing this process a long time before we decided to put this security layer on it, and if you get that for our regional point, you have to be transparent to commerce, if you aren't, what's going to happen is this, you change their process and now you are slowing their capability.

Figure 13: X-Ray Scan of Truck in Rotterdam

This is a very interesting thing and let us talk about this for a second. I am doing a thing called Project Neptune. We are working with a couple of partners, and what we are doing is taking a real-time image of containers going through the port of Rotterdam, this picture was taken on the 6th of August, it was transmitted in the morning of the 6th of August in Charleston, South Carolina and then shown to the Transportation Security Administration conference there, that is our first step, the next thing we are doing is this, this is nice, where do you want to add value to the governmental customer? Let me explain the process right now that goes on, if you are in the Netherlands and you are looking at these container pictures, there are three human beings that have to look at a picture before that container can get through, that takes about 20 minutes, that is ridiculous. Also, US Customs is spending an inordinate amount of energy to deploy inspectors to oversee these locations. We think you take these pictures in foreign ports and right now we are working with some folks in the medical industry, because the medical industry for years has had software that does analysis of x-rays, so we are working with some guys in the medical industry who have a lot of experience doing x-ray analysis. They can figure out in these x-rays what are anomalies that lead you to need to do some type of inspection on this container. We think something like this, you take these things, you encrypt the picture overseas, use a high-speed data network to send them back to a customs base here in the states, run through the software, process, it pops out five or six of maybe 100 containers that need inspection, then you notify back to either the single US Customs agents who is over there (vice the five or six now over there) who is working in a bilateral arrangement. You start that way and then you start doing it the other way so that they can get, they, maybe Rotterdam gets the same deal out of US Customs, now here is one of the challenges you run into on this, we worry about the terrorist stuff coming into the United States, have you ever talked to Dutch customs? It is not on their radar screen, they are in the revenue collection business. What they want to do is find contraband, so in addition to finding terrorist thumbprints on these things, we look in things that will help in the detection of contraband. We think that is a very simple solution that is realizable today by using literally modifying some cop software to do this stuff, the encryption software,

you'd be very interested to know where we got it from, you take this picture like this, this standard, that is about 100 megabytes ok, so that is going to clog most networks, so you have to do something to encrypt it and compress it, the reason you have to encrypt it is the bad guys will figure out you are doing this and they'll change the picture while it is undergoing transmission, um, we have a company called Digital Cinema that takes films from Hollywood and it digitally sends them out to people, a two-and-a-half-hour movie is a huge data chunk, we have some very advanced compression technologies we've developed to compress those movies, we are using the same thing here, so what we've found is by using those compression technologies, 100 megabyte picture gets down to about 2 megabytes, which is much more usable on a network ok,

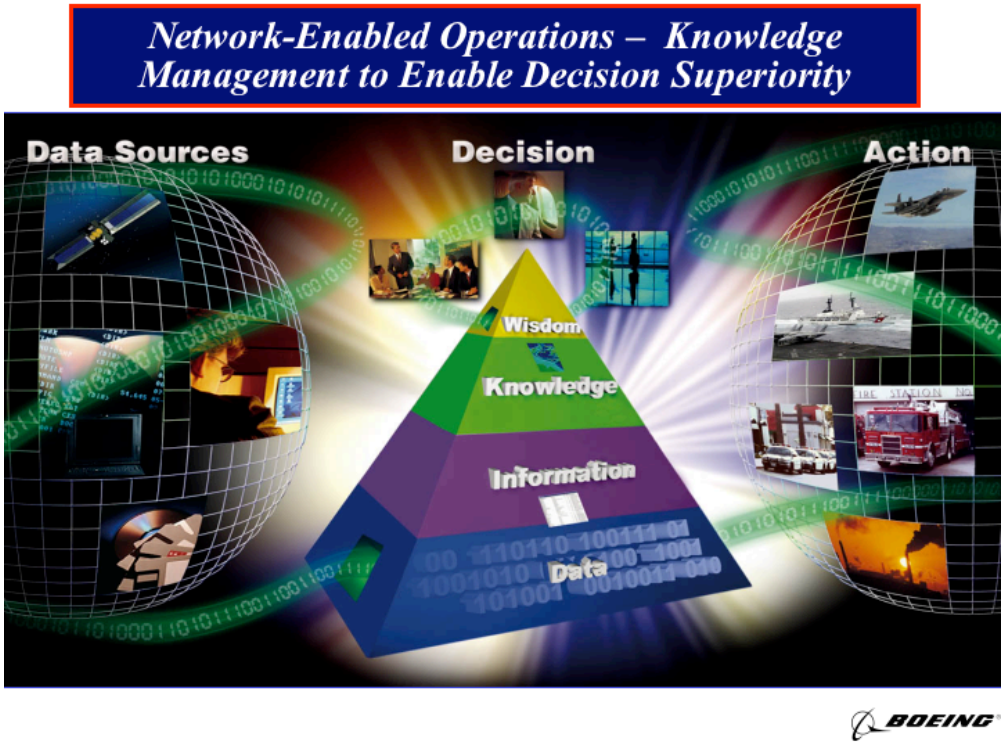


Figure 14: Network-Enabled Operations

The short answer, we are in the process of doing this, we are working with Customs. I have a couple of meetings coming up, we've done some stuff already, we think this is realizable, and we look at a governmental customer, one of his biggest costs is manpower, this allows him to make better use of his manpower base. In the homeland security domain, we think this little box here getting you from data to information is when it all becomes decision relevant in the current battle, we think knowledge is what you collect out of there, and that is how you fight the future battle for risk assessment engines, if you don't have both of those things working for you, we think you are probably not going to win over the long run or you'll be extremely vulnerable to some type of incident.

Figure 15: A Comprehensive Solution

What's the road ahead, where are we going and how do we get there, I want you to just take a look at this, this kind of covers the things I've been talking about, the short answer is, you have to take care of a commercial customer, you have to take care of a governmental customer, yes in fact these folks do have intersection and a Venn diagram, the commercial customer is keenly interested in doing this, why? Because he sees this as a way of entering into a partnership that allows him to continue to run his enterprise without being subject to draconian rules, the government, TSA, customs, those type of folks, they are interested in this because they also realize that, particularly customs, they are kind of have an internal conflict of interest that is been solved a little bit by DHS, they are responsible for collecting revenue for imports, which conflicts with the goal of maximization for velocity of cargo, at the other end of the spectrum, so they are always trying to find this balance in the middle. This allows them to work toward that balance, it also allows TSA to use a very limited manpower base that they have working on the land and maritime arena to solve this problem because if you look at what they've got working on land and maritime compared to airports, it is fractional, below the 5% level, so there is a big manpower tradeoff there.

Figure 16: The Road Ahead

This is my basic message, what I think is my call of action, what do we need to do now? We need to look at this in terms of physical and data-centric layers, we've have to avoid the single point of failure solutions, we build it into a relevant decision support environment because you are going to try to use machine-to-machine decisions wherever you can, but ultimately, humans are part of this process and play directly into the decision, in the decision making rule, you have to stay ahead of the asymmetric enemy, why? You know what? Part of the challenges of living in a free society is CNN reports almost everything we do every day, that is one of their best data collectors if you are Osama, he is using that as an, it is almost like having your own intelligence collection facility, it is have to be commercial and governmental partners, we've have to get that information, because the data's out there, it is just a function of properly capturing it, transforming it, and putting it in front of decision makers, I have probably spent about an hour here talking to you, and you know what, I don't like to talk that much, so I'd like to open it up to questions now, yes sir.

In the early part of your talk, I perhaps misunderstood something so I want to check. You showed a slide about a strike at the Port of Long Beach, and the inference was that that was equivalent to a terrorist activity, if that is what you meant, I would also like to ask whether you believe that the scandal we had with Enron at about the same period of time where a number of Americans or a large fraction of Americans were threatened with access to the power grid also represents a terrorist activity,

That is a very interesting question and I'll answer it directly, now the first thing is, the slide you mentioned actually portrayed an entire West Coast strike that occurred for 10 days last Fall, so it is more than just the Port of Long Beach, no, you should take no inference that that is a reflection of what a terrorist incident might be, and I will tell you your last question of Enron is completely inappropriate for me to comment on that, I have no intention on commenting on that, next question please, yes sir.

Could you talk about the privacy issues involved? I noticed that that important topic wasn't mentioned.

Let us talk about two things, privacy and liability. Um, I am really happy to work in maritime commerce, you know why? 20-foot containers don't have any civil rights ok, now that sounds like it is a humorous thing, but it is actually very serious, how may of you in here are familiar with a governmental program called CAPPSS 2? Ok, CAPPS 2 is a passenger profiling system, the Transportation Security Administration awarded it I believe in April of this year, and really what it is, it is a passenger profiling system to find bad guys, ultimately, it would far preclude the great majority of people sitting in this room from being wanted by a TSA screener and all the other things like taking your shoes off, because what it is intended to do is take those crumbs of data that I talked about before and pick out the people that have a high potential for probably doing incidents against the US economy and government, I think it was awarded in April, right now, if I am not mistaken, there is still two more scheduled senatorial hearings on it, There is a GAO study that has to be done and there are several ACU suits that still need to go through the process on it, so what you run into if you are dealing with citizens, US Citizens, there is huge privacy issues ok, now, let me transport you about 6,000 miles here to England, I've been doing some work with, I found it, this is kind of enlightening, in England, they don't, this privacy stuff is, profiling, bring it on, cause in England you are not a citizen, you are subject to the crown and the crown determines what is for the best of society, so in England, BAE said we have no problem with those profiling rules here for our air passengers, so there is a clear difference in our form of government, now, that deal, what's really, you want to hear privacy, you are predominately dealing with human beings, if you are dealing with inanimate objects you deal with intellectual property, and generally it is a lot easier to protect, so did that answer your question, ? This is an example of a tough nut to crack, now let us talk about the other thing of liability, um, this has been a very interesting thing and adventure we are into here because we think we are going to add some value to both commercial and governmental customers, what if we fail as part of the process and there is an incident? Then the question becomes, basic no commercial enterprise in America could handle the liability associated with this ok, so there is several legislative things going on right now, let me give you the current and the future, most of you who flew here did you have to take your luggage and put it through some large machine or did somebody swipe it on stuff? If you did, you probably didn't know it, you know who put those machines in the airport? Boeing did, before Boeing put those machines in the airport, they examined this liability issue in great detail, in, in great detail, and we have coverage from a corporate level under a thing called the US Safety Act ok, because we cannot completely guarantee everything, simply because, for numerous reasons. So EDS machines, explosive detection systems and covered under that, this entire maritime cargo business, this doesn't fit neatly under the US Safety Act, there are some bills that started not long after the 11th of September to cause indemnification of homeland security solution providers, they are kind of bogged or dead, um, that is a large issue because, I will tell you, a lot of people tried to enter this market originally because it looked like it was this, you know, this huge market, and when you start looking at it in detail and you look at this liability thing, uh, you have to examine it pretty closely because if you fail, you have some huge corporate risks in front of you, the other thing is, you have entered into a partnership with the government here and you have really let down your partner in a manner that could never be recovered, so there is two things, there is privacy and

there is liability, I had never thought about this before, unfortunately now I probably spend about a third of my time with lawyers learning about this so, and Tony knows all about lawyers from some comments yesterday, next question, yes sir,

It looks like that you are dealing or focusing on supply chain security as well, does this also include non-supply chain situations, for example, the international movement of household goods that involves self-packaging, self-packing that sort of thing, or not?

Well, that is a very interesting question and let us, let us tell you where we are going with that, the way we kind of view this thing is it is an elephant, and we are careful when we bite off as much of it as we can eat at a time, right now we are focused on containerized cargo, there is no doubt about that, where are we going? The next thing we are probably going to go after, there is two big, from a corporate perspective but the US Government, when you look in this domain space, the next thing that is have to be solved, this is the thing that unless you live in Washington State or New York City, probably doesn't hit on your radar screen, coastal ferries, here is what the problem is, you have a coastal ferry, you put maybe 100 people on it and 40 cars, and then it pulls up to a nice little pier in New York to off-load, you know what, 40 cars, each got a half a tank of gas, man, that is a red letter day if you are last name is Osama ok, so that is the next thing they are going to go after. Commercially, let me tell you who is clamoring for this, would love it, automobile companies. If they ship their cars on non-secure ships, in other words, they don't own the whole ship, then generally they are losing between 33-50% of the cars coming off that ship so they've got a big stake here, they are very interested in this, the other people that have studied well ahead of this is the oil industry, why? They have a larger problem because of the nature of their cargo, and they are using some completely, they are securing their supply chain, but they also realize at the point of debarkation they had better take some unusual approaches in order to secure their product, so, I am looking at this port right now, the oil industry is well down the turnpike, here is why, you know the oil industry is well down the turnpike. Operation Safe Commerce grants from Transportation Security Administration, most of them were anywhere between maybe $1 and $4 million, except one of them, they went to Exxon-Mobile, it had to do with securing an LNG facility into a pipeline, that was a $24 million grant, why? There is a huge potential, if you blew that thing up, the state of Louisiana basically has a new canyon in it ok, Tony have I, have I exhausted my time or, yes sir one more question.

Let me ask this question in the following way, how will you know if you are being successful.. and let me give an example of uh, perhaps a metric. There is lots of contraband that comes into this country, if you are being successful, then wouldn't you hypothesize that the amounts of contraband coming into the country should dramatically drop, and if it doesn't, then are you really adding any value because there is huge amounts of things that are being missed.

A very good question and let me uh, explain how we are approaching that issue. Your question assumes that you want to do everything right from the start. Our approach assumes that the first thing we want to take care of for the governmental customer is absolute prevention of a terrorist incident. While we do that we get some concurrent spin-off in contraband material, that is great. The first thing we have to do is prevent the terrorist incident, that is a non-negotiable mandate. We will evolve over a period of time further abilities to go after contraband, but it will never be at the cost of preventing a terrorist incident, so while we may have a tiered group of attributes we

offer in this product, this first one is at the absolute priority and takes 100% priority over everything else in the governmental customer, and now let us go over and talk about the commercial customer because you know what, that is a lot harder guy ok, he, he is got reverse contraband called shrinkage ok, and he doesn't like to talk about that in public for numerous reasons, we believe that we have to demonstrate the ability to reduce shrinkage, increase his in-transit visibility and allow him to basically have some ability to control velocity in that supply chain, that we believe is very measurable, and those three things because of close relationship can be done at once, the contraband thing though, it is secondary, it is very clear when we talk to foreign governments they are interested in that, but as far as our #1 customer which make no mistake is the US Government, we are going to take care of the terrorist incident thing before we go after contraband, I don't know if I answered your question but that is kind of how we look at it.

My point was that if contraband gets in, then terrorist devices could get in.

That is an interesting point, but that assumes the attributes of the contraband equal those of terrorist devices, in some instances that may be the case, but in general, once you start drilling down into this, you find in fact there are some what I call data level significant attribute differences, so,

Thank you very much, I appreciated the opportunity to talk to you today.

A Paradigm Shift for Information Technology

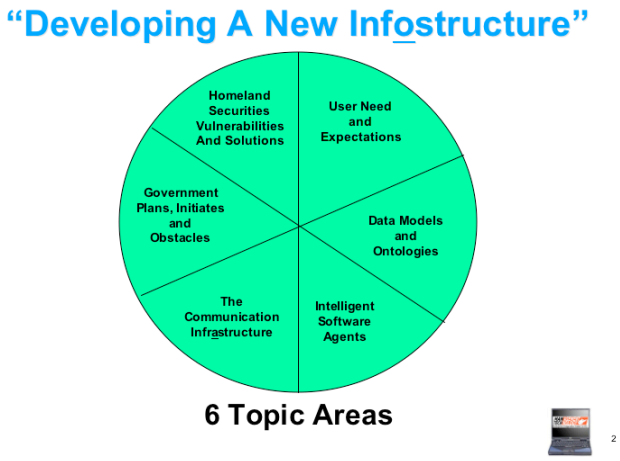
Robert Kidwell
Vice President
ManTech Advanced Systems International, Inc.,
Fairmont, West Virginia

Well, good morning ladies and gentlemen. I am delighted to be part of this two-day conference. I think the briefings up to this point certainly have been more than adequate and right on target. I titled my briefing "A Paradigm Shift for Information Technology" because I am an IT guy and I think that we have got to get it right this time and we have got to do certain things in a better way as we go into the future. So I based my premise and my entire briefing on the pig and the sow.

There was this guy in Los Angeles who had a cabin up in the hills. Between him and his cabin there was a very dangerous curvy road, but he had a 911 Porsche so he didn't care. Every weekend he would drive out to the cabin in his Porsche. I believe he was an attorney, probably the same guy that Tony Wood mentioned yesterday. He was on his way to his cabin one Saturday afternoon and he was coming up to one of the hairpin turns so he downshifted his Porsche, getting ready to get himself into the turn, when all of a sudden a car came out of nowhere from the other direction and almost careened right off the cliff. Then the other driver got a hold of the car and it came back and started heading towards him. So the guy stopped his car and he said, "my God it is going to run into me. We are going to have a terrible crash." At the last instant the other driver got control of the wheel, straightened it up and went down the mountain. As they went by, the woman yelled at him "Pig!" So not wanting to be outdone by this woman, he shouted back "Sow!" as he put his car in gear; he was pretty happy with himself that he had not let her get away with anything. Then, he went around that hairpin turn and ran into the pig.

So my premise is, if people say things to you, then stop and ask them what they mean. Interoperability is a goal. Interoperability means different things to different people. Now, Mike Sang gave me the best example of that. We have in IT that interoperability is disparate systems that seamlessly transfer information, context, and understanding in a loosely coupled

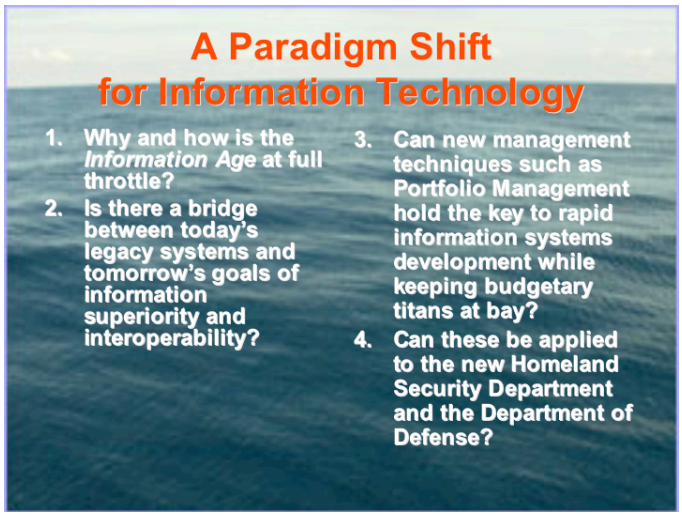
environment. The C4ISR is the only document I have ever seen in DoD that actually addresses five levels of interoperability, but that is where we all need to go. Next slide, please.



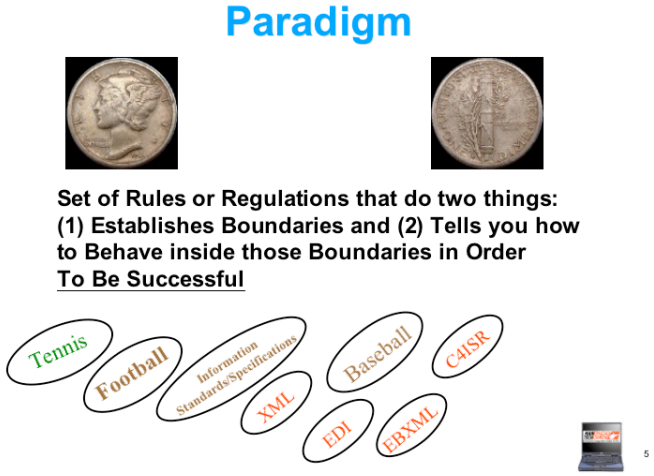
Now Jens gave all the speakers six topics to address in our briefings. And as I said, the speakers have all been on point. They have all addressed a lot of issues. The one that I think we have got to focus on more is user need and expectation. I come from the era where when we developed applications with users, we began to think that we knew more than the user did about the application. And so we would implement something that met maybe only 70% of their need. Then we got to the era where we said business process re-engineering and that sort of implied that the process was engineered right the first time, certainly not always the case. If you go up and down the Pentagon and many government agencies, you will find out that they will say it is the process that is stupid. I'll say no it is the data dumbbell, because one without the other just doesn't work. You can eliminate all the process in the world, but if you do not have the underpinning data, then you are not going to be successful. So, you have to put the two together. Next slide, please.

So my premise is that I am going to utilize four questions to highlight some of the paradigm shifts that we have occurring within the federal government and the IT community, particularly

in DoD and also some thoughts on the future. I fully realize with the few minutes that we have got together we will not have a lot of time for in depth coverage, so please feel free to e-mail me at kidwellr@mantech-wva.com. The WVA is not a foreign country, that is West Virginia and you will see why I have been banished from West Virginia in just a few minutes. Next slide, please.

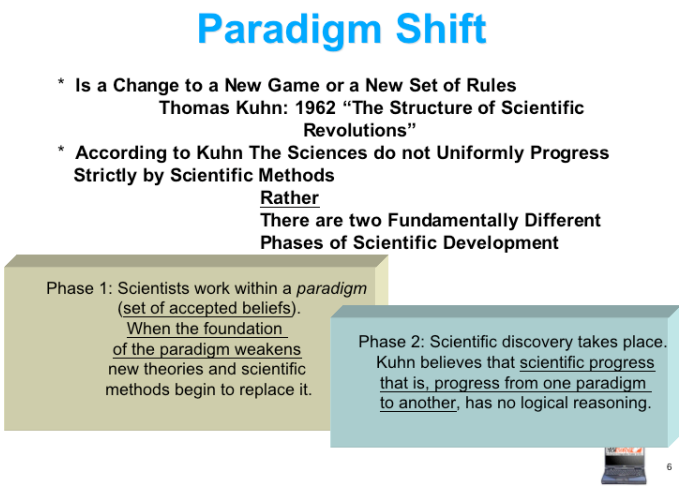


My four questions are these: 1) why and how is the information age at full throttle; 2) is there a bridge between today's legacy systems and tomorrow's goals of information superiority and interoperability; 3) can new management techniques such as portfolio management hold the key to rapid information system development while keeping budgetary titans at bay; and finally, 4) can these be applied to the new Homeland Security Department and the DoD, Department of Defense? I'll try and cover those very quickly. Next slide, please.

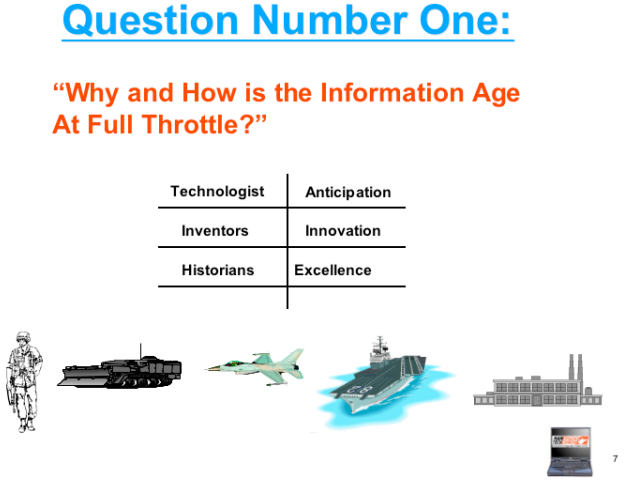


Paradigm. I like definitions. A paradigm is not 20 cents, it is not two dimes. It is a set of rules and regulations that do two things: 1) it establishes boundaries and 2) tells you how to behave inside those boundaries in order to be successful. A couple of simple examples are a tennis match when it is 45-love or there is 6 to 4, you have to understand those rules and regulations in

order to understand and watch a tennis match. But that is really a paradigm and if they apply those rules and regulations inside, they will be successful; you have a winner and you have a loser. So there is a very quick order of what a paradigm is. Another example of a paradigm is football. Also, we have information standards and specifications if you follow these, (i.e., XML, EDI) they are paradigms. If you follow those rules and regulations, then you will be able to successfully exchange information with each other. We are shifting all the time. Next slide, please.



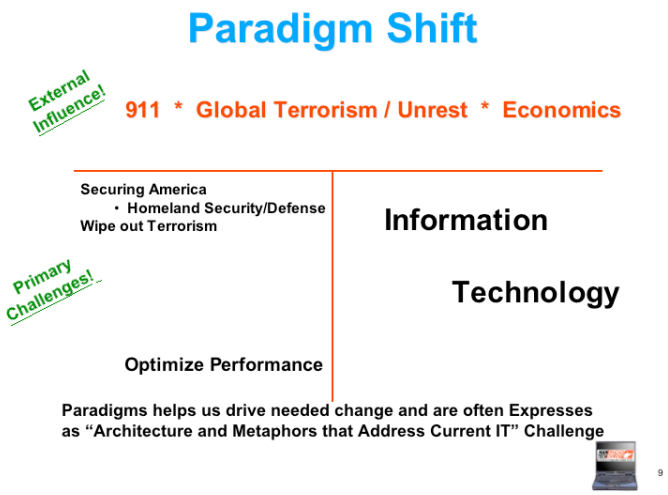
So a paradigm shift is a change to a new game or a new set of rules. Thomas Kuhn, who wrote the Structure of Scientific Revolution, actually coined the term "paradigm" and "paradigm shift". He said it could only be applied to the scientific community, but I disagree with that. It can be applied to the social, culture, and certainly our technologies. But, if you listen to his description, phase 1 - scientists work within a paradigm which is a set of acceptable beliefs and when the foundation of that paradigm weakens, new theories and scientific methods begin to replace it. This is where we live. This is who we are. This is happening every day and usually there are external influences for that paradigm shift. Scientific discovery takes place, and he believes that scientific progress from one paradigm to another has no logical reasoning. Next slide, please.



So question #1: why and how is the information age in full throttle? We have technologists like Bill Gates and others that write books anticipating the future. They tell you what they think is going to happen and what is going on. We have innovators or inventors, certainly Steve Jobs when he invented the first Mac and the PC world revolution took off, who do not wait for these pontifications and so forth. Then we have historians like Nesbit and so forth who write about excellence and project what they think the future will be based on and what the past looks like. Next slide, please.

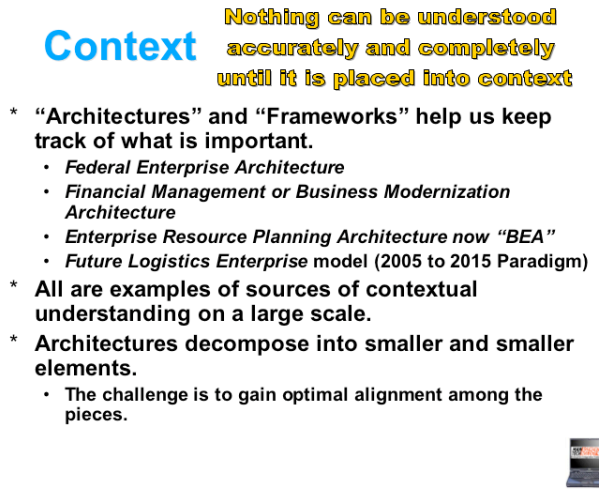
Now, what is driving change today? Of course, today is a very poignant day and a very respectful day. Certainly national security, terrorism and global security are our #1 priority. The American economy and the global economy are right behind them and as our keynote speaker said this morning. Another is the aging workforce. I chaired a session about six months ago where I said I am an IT guy; I have been at it 30 years and I have been fortunate enough to work on the cutting edge with a lot of technologists. I also said that I hope to spend a lot more time in the future than I have in the past. One of my guys in the back of the room told me at the break, "Well Bob I added up the numbers and it just doesn't work." So we all got that issue coming up.

There is unprecedented coordination between our federal, state and local governments. Every company doing business with the government has created a Homeland Security Division or Unit. We at ManTech did not want to be outdone. We have a National Security Solution Group. There are two things wrong with that: 1) National, it's really global; and 2) Solution, you know as our keynote speaker also said and I believe it, there are no real solutions yet. There is some wonderful technology and wonderful things we can apply, but there are no solutions to Homeland Security yet. Next slide, please.



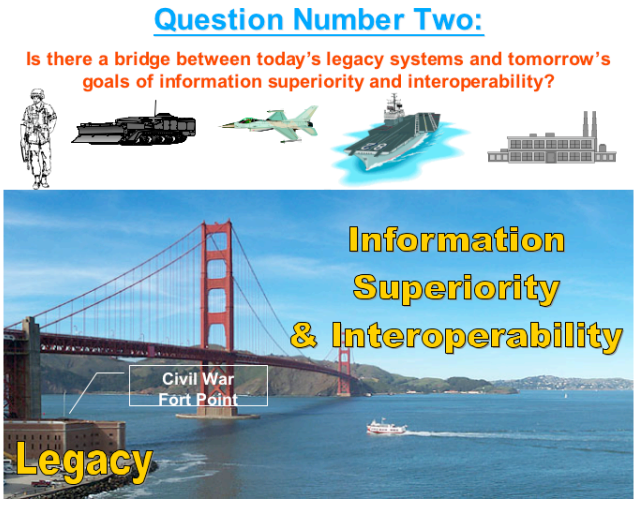
So the paradigm shift is external influences, primary challenges, and securing America. The number one priority is wiping out terrorism and then you can fill in the blanks to optimizing performance. Paradigms help us drive needed change and are often expressed as architecture and metaphors that address current IT challenges. My message is that we in IT have a chance to make things right for the past; we have a chance to really have a tool kit that has all of the tools necessary in order to do a job to meet you as the user's needs and requirements which is something I believe we have not fully done yet in the 30 years I have been at it. Next slide, please.

So paradigms help us manage to secure America, to optimize performance by identifying what must be managed, and providing ways to think about performance management. But often it leads to process performance improvement. Next slide, please.



This is the word of the conference and I am no different. Context. Everybody has mentioned it, but nothing can be understood accurately and completely until it is placed into context. Architecture and framework help us keep track of what is important. These are some of the initiatives that we are involved in to DoD and the federal government. The federal government has a thing called the Federal Enterprise Architecture. How many people know about that? What it is doing is it is going to put out a series of reference models starting with the business reference model, performance reference model, technical reference model and it is a support for IT work in the federal government. In the DoD, one of Secretary Rumsfeld's top issues is financial management or business enterprise architecture and that BEA should be up here and not down here. Enterprise resource planning or ERP SAP, there are five programs in DoD right now that use the ERP SAP. It is going to have a large impact on our landscape in DoD. The future logistics enterprise model, how many people know about that? I will speak about it in a couple of minutes, but the FLE is the future logistics enterprise model for the Department of Defense. All of these are examples of contextual understanding on a large scale. Of course architecture as we know can decompose in smaller and smaller elements as time goes on. Next slide, please.

So I think that to answer question #1 we are certainly in full throttle in the information age. We are commanding some significant resources to advance progress with IT as fast as we can because we believe it is producing desirable outcomes and can be even more productive as we go forward. There is no element of our society that does not have an IT component at the very core of what it is trying to do, including Homeland Security, Homeland Defense, Global Security and so forth. Next slide, please.



Question #2: is there a bridge between today's legacy systems and tomorrow's goals of information superiority and interoperability? Information superiority says that we will get the right information to the right user in the right format at the right time. It also says that we will provide information in a certain way and deny our adversaries the access to that information. There are two levels to information superiority. Next slide, please.

I want to talk a little bit about semantic framework mediation as an emerging paradigm with a strong future towards interoperability. It has applicability to both Homeland Security and in our Department of Defense. Next slide, please.

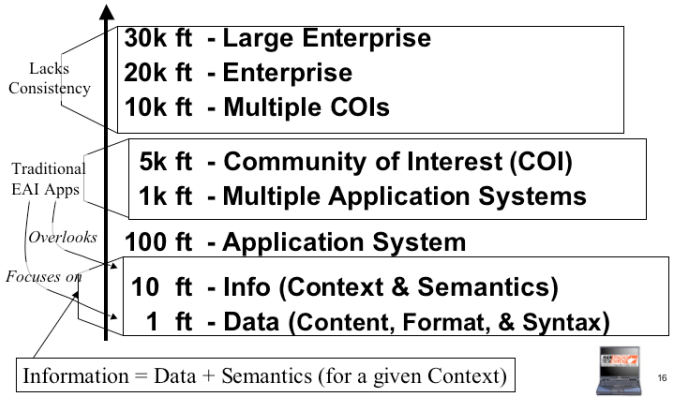
What are semantic mediation and semantic interoperability?

* Semantic mediation describes the process of translating terms and their use in context from one set of user views to another set of users in their own unique context.
* In this regard, the same terms may not always have the same meanings.
  - Different terms may be used to describe something, and understanding is always derived from interpreting in context.
  - Semantic interoperability describes the outcome.
* Yet, the ultimate outcome is information processability whereby computers perform work automatically while accommodating different users, operating in unique contextual environments, with their own terms, rules, and infrastructures.

15

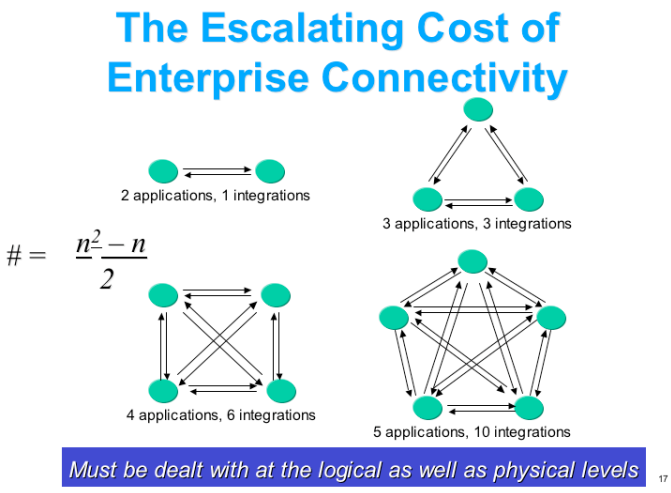
Semantic mediation is simply a way to describe and translate terms and their use in a context form from one set of user for use to another set of users for use in their unique context. Next slide, please.

Interoperability – 30,000 ft View: "*Observations from the ground up*"

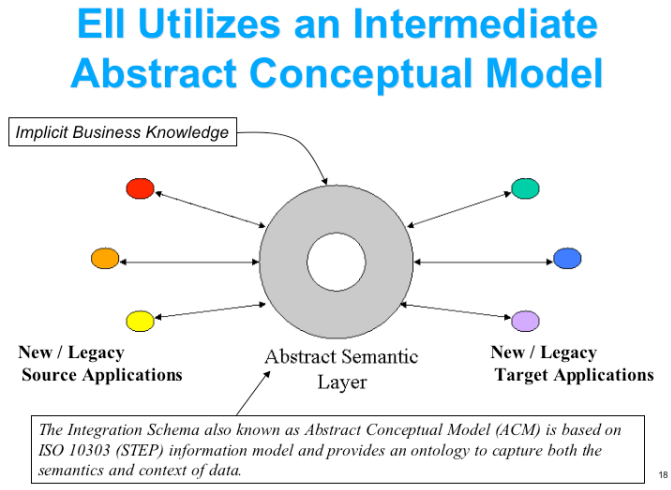


16

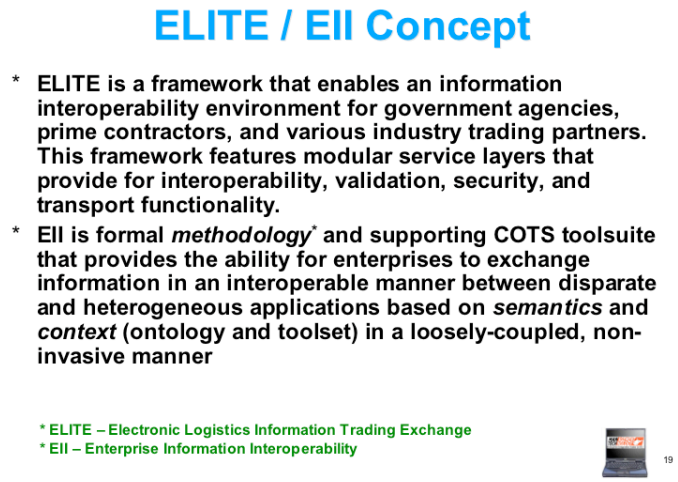
This is what I call the 30,000 foot view. We start at the bottom where we start with data; we have content, format, and syntax; moving on up we have information, which is in context in semantics; then we get up into the application systems; multiple applications systems and we get here with what we call a community of interest. Take XML for example, somebody asked a question yesterday about XML's name space. An XML name space is to communities of interest just like you have in DoD, we are looking at domains for logistics acquisitions and so forth. So community of interest is a very important level to achieve. Then you go up to multiple communities of interest and finally you get to the enterprise and the large enterprise. When you talk about Department of Defense or Homeland Security, you have to talk about that department as an enterprise. This is what makes up those enterprises. Next slide, please.



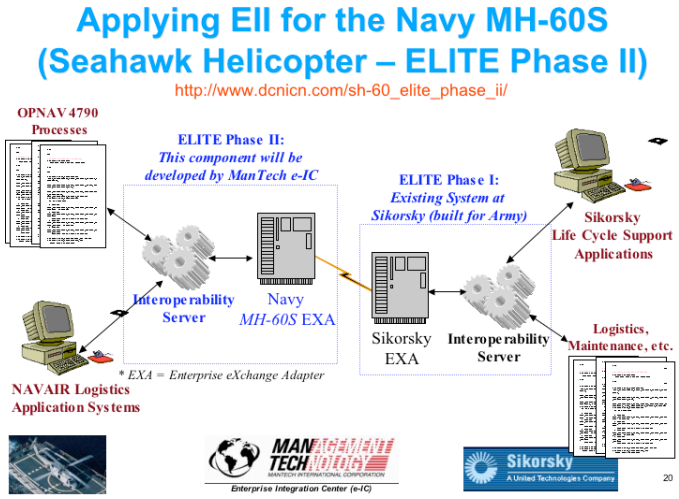
Now today we have this problem called N-1, where we have hard coded real interfaces between our applications and it is called EAI or Enterprise Application Interface is the term. The Defense Logistic Management System or DLMSO has 12,000 interfaces alone in their system. DLA spends 80% of their software budget annually on maintaining the interfaces, not the applications. This is a big problem. ERP SAP will generate thousands of interfaces for DoD alone. One of the alternatives we are looking at to this approach, next slide, please, is what we call enterprise information interoperability or EII and what it does is it builds an abstract semantic layer in a neutral format so that people can exchange information in context and meaning. Can you go back a slide for a minute? So we are trying to go from this, where I have to maintain all of these N^2 interfaces to something that is a doughnut that is in neutral format. Next slide, please.



It is an abstract semantic layer. It is based on the ISO STEP information model and provides ontology to capture semantics and context of data, a very powerful thing. We have been working on this for the past 18 months and it has a lot of problems. Next slide, please.



We are part of a group working with DoD that is called Electronic Logistics Information Training Exchange or ELITE. ELITE is a framework that enables information interoperability environment for government agencies, prime contractors, industry trading partners, etc. It has very big potential. Next slide, please.



We are building a pilot project between NAVAIR and Sikorsky where we are using this tool to see how we can bring interoperability between the prime vendor Sikorsky of the MH-60S helicopter and its prime customer, which are NAVAIR and the US Navy. We have metrics and things that we are going to use to give ourselves a grade as to how well we achieve that program. Next slide, please.

Emerging Commercial Tools for Enabling EII / ELITE

* **Modulant Solutions - - - - - Semantics Mediation**
  - **Contextia Toolset**
    - www.modulant.com
* **Microsoft**
  - **BizTalk Server Enterprise Edition**
    - www.microsoft.com/biztalk
* **MetaMatrix**
  - **MetaBase and Modeler**
  - **MetaMatrix Server and XA Server**
    - www.metamatrix.com

21

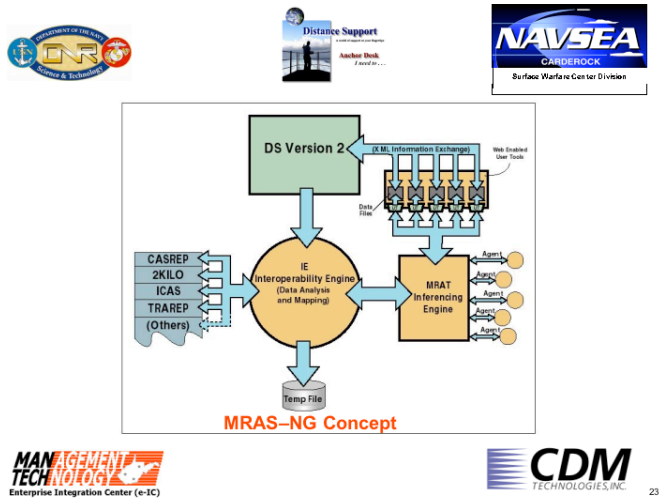
These are some of the products that we have been working with and assessing. Modulant is the organization that has the semantic mediation tool and they are located in South Carolina. Now the problem that you have with some of these tools is that the resources you need to train and get educated on how to use these tools properly is not a small investment. So, we are going to end up with a lot of specialists over time having to do with what kind of tools or products that you use for limitations. There is talk from Microsoft on meta matrix. This is a little different wrinkle that works strictly with metadata, but it will take the metadata across the enterprise and put it into a standardized kind of format for you. Next slide, please.

Semantics Framework/Mediation Emerging Paradigm Coupled With Intelligent Agent Emerging Paradigm to Provide Critical Decision Support

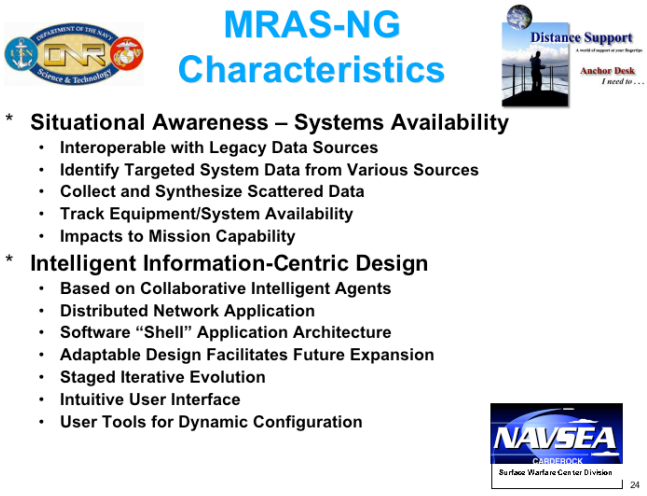
"Riding the Waves of Technology"
MRAS-NG

22

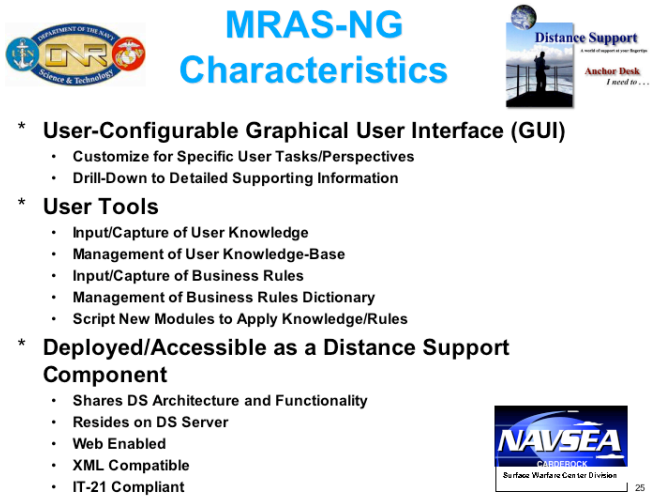
The next project I am going to talk about is also semantic framework mediation, but it's coupled with intelligent agent emerging paradigm to invite critical decision support. One of the most pressing problems our Navy is faced with in the future is its precious resource of its men and women in uniform and on board ship. How can we devise a decision support system that will aid and abed the commanding officer and then ultimately the battle group and the tide commanders, where their very precious resources at its ultimate minimum, and that's what we're trying to do here. We have a program called SILS, which is a shipboard integration of logistic systems and Mission Readiness Assessment System -NG is our next generation. Next slide, please.



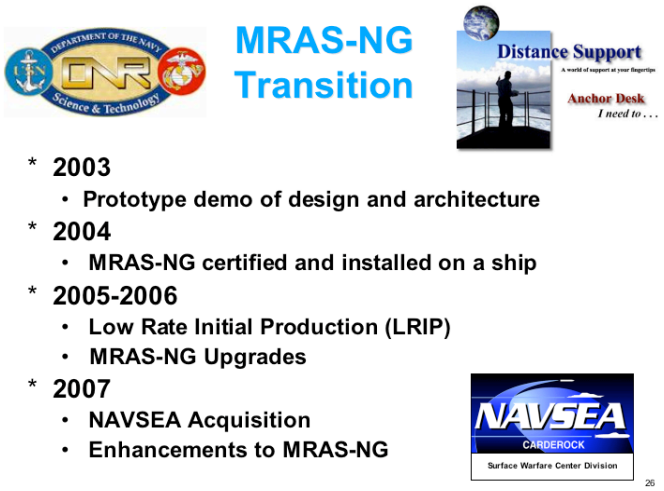
So what we are doing is building an interoperability engine to interface with all of these legacy databases. We are building a software shell and we are using CDM as our partner with their reference engine with agent technology. These will change and grow. We are building a very simple shell that ultimately hopefully will go aboard every ship. Now someone made the point yesterday, I believe it was our keynote speaker from yesterday and he said that everything must go through the normal process of becoming a program of record. What we are doing is we are transitioning from ONR to distance support in the Navy sea system command as a program of record. That means we have to go through the bandwidth issues, software licensing issues, performance issues, and all the things that normal programs have to do in order to be successful out on a fleet. So we have our work cut out for us in the next year. Next slide, please.



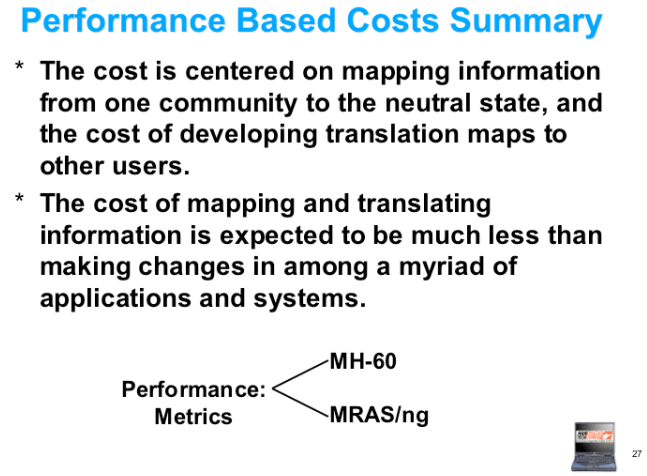
This is some of the capabilities that we are going to instill in the commission assessment readiness assessment system. It will be intelligent-centric design based on collaborative intelligent agents and our interoperability engine. Next slide, please.



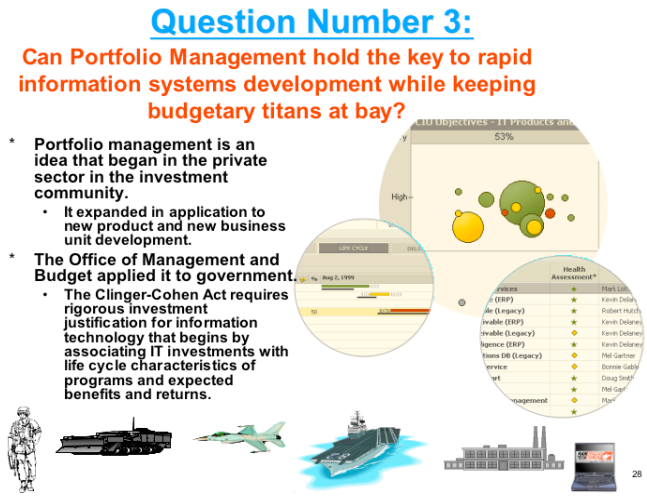
We have a set of tools, user development tools and user application tools. We hope to deploy it via the distance support program out into the fleet. Next slide, please.



This is our schedule. It would be great to come back next year and give you a report on the MRAS next generation program because it does involve and embody interoperability. It does involve intelligent agents and certainly legacy systems and how we are going to move that paradigm. Next slide, please.

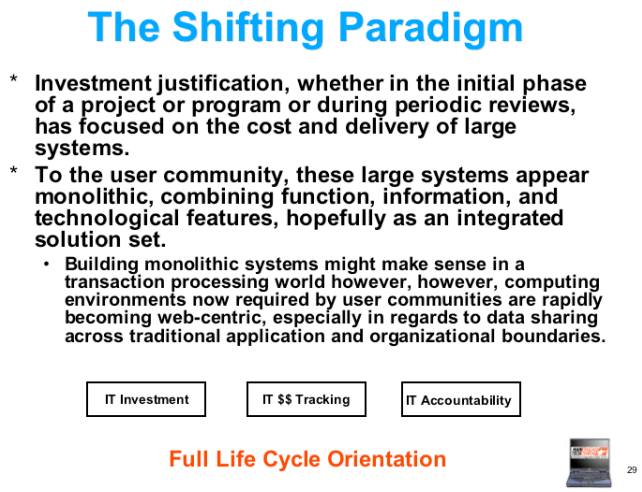


For each of these programs, we are trying to give ourselves a grade. We have performance metrics we have put into both of them. Next year we should be able to report to you on what we are doing with them. Again, this is going to drive the metrics which will drive the cost, and that is ultimately very important. Next slide, please.

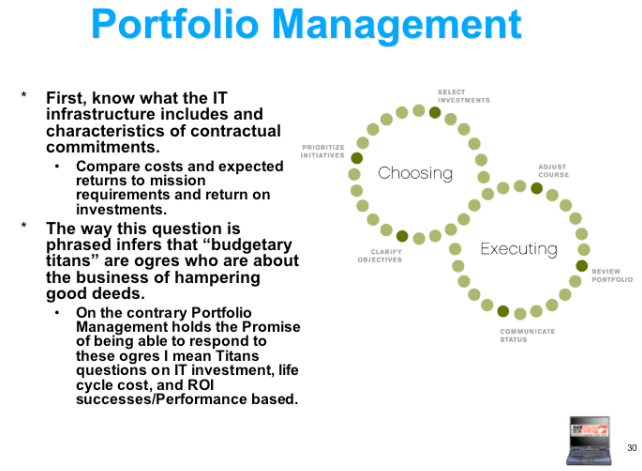


Question #3: Can portfolio management hold the key to rapid information systems development while keeping budgetary titans at bay? Does everybody know about portfolio management? It comes from the investment community, not Enron or Worldcom or any of those guys, but it is a tool for diversification and it allows you to define your requirements. It allows you to track your assets and to track your products that have those assets as components. It is an idea that as I said began in the investment community. They expanded the application to new product and new business development. OMB has run several programs with it. It is based on the Clinger-Cohen Act, so it has some of the drivers of the Clinger-Cohen Act embedded into it. You are going to hear this term more and more as the government goes forward, particularly in Homeland Security, as well as in the Department of Defense. The Clinger-Cohen Act requires a rigorous investment justification for IT that begins by associated IT investment with life cycle

characteristics of programs and expected benefits and return. Portfolio management is the animal that will do that for you. Next slide, please.



So the investment justification, whether during the initial phase of a project or during its periodic reviews, portfolio management can play a major role. One of the things we have always been accused of is the value of computers. Can I really track my IT assets; can I really determine its value; and can I really determine its accountability; and therefore, can I really determine a return on life cycle investment? This is a very tough challenge and portfolio management is key to doing this. You will see that OMB will be more and more structured in the way it is going to do business case analysis and business case management. This is the way that you are going to have to go in business case models; you are going to have to go on this path. So we in IT have to be not just technologists, we have to know how to be successful. Next slide, please.



So you first have to know what the IT infrastructure or your architecture is, including the characteristics and your contractural commitments. The way I posed the question inferred that the budgetary titans who are over us are about the business of hampering good deeds. I personally think that, but that's another matter. On the contrary, portfolio management holds

promise of being able to respond to these ogres', I mean titans, questions on IT investment, life cycle cost and return on investment and your success on performance based activities. This is where everybody is going in the government. Next slide, please.

Question Number 4:

Can these be applied to the new Homeland Security Department and the Department of Defense?

* **Information interoperability strategy, methods, and technologies can be applied to exact higher return from IT investments, beginning with legacy systems.**
* **Information interoperability strategy can be employed as a primary catalyst for change and improvement, yet this must be differentiated from traditional approaches that are aimed at standards-driven sameness versus a less invasive approach.**

31

Question #4: can these be applied to the new Homeland Security Department and the Department of Defense? You know again as our keynote said this morning, there are 22 agencies. They each have their own culture, their own rice bowls, and their own IT philosophy. In order to extract what you need from each of them in a way that would make sense to a department, you are going to have to go to interoperability as a baseline. So again, I think IT is going to play a key role in homeland security. Information and interoperability strategy is going to play a key part of that. So, look out for it. Next slide, please.

Applications

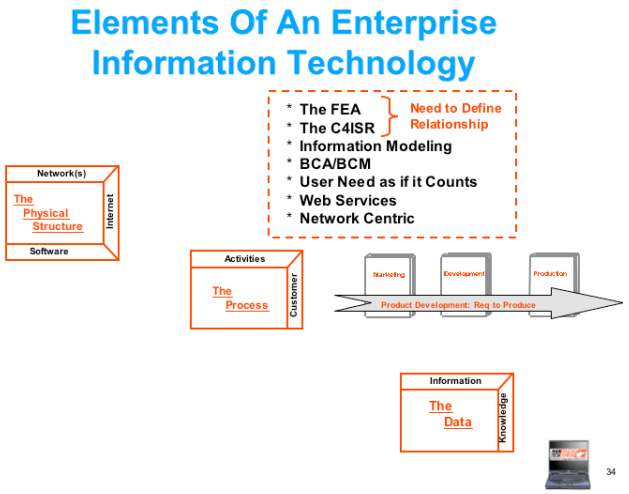
* **Portfolio Management technology can be applied as a starting position for both the new Department of Homeland Security and established Department of Defense.**
* **Application of these ideas should be accomplished in context with a Management Approach that accounts for four performance dimensions:**
  1. **Leadership and Integration,**
  2. **Processes and Knowledge Management,**
  3. **Enabling Mechanisms: People and Technology, and**
  4. **Time and Capacity for Change and Improvement**

32

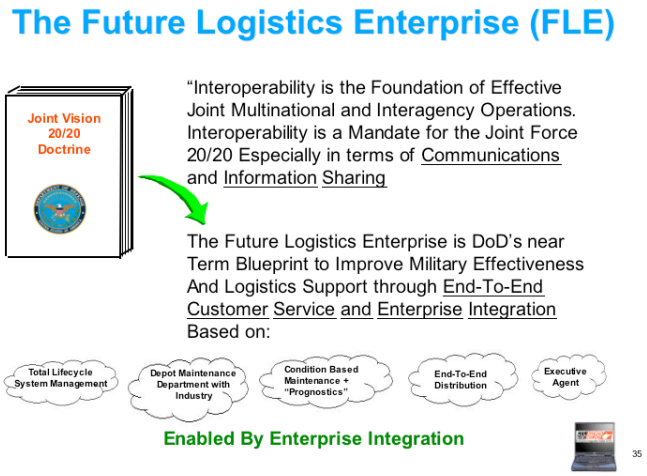
Portfolio management technology can be applied as a starting position for both of these departments. Applications of these ideas should be accomplished in context with a management approach that accounts for four performance dimensions of leadership and integration, process and knowledge management, enabling mechanisms, people and technology, and time and

capacity for change and improvement. All are very important issues. But you will see that portfolio management will begin to rise up in all of these departments.

Now a few summary points from my paradigm shift for information technology. Next slide, please.



These are the elements of an enterprise information technology. We have our physical structure, our software, internet, networks, the process, activities, customers, and we have the data, information, soon knowledge, and I always leave wisdom off because I will be long gone by the time somebody deals at the wisdom level. OK, we are still dealing with data. You have the "FEA", the C4ISR is where we live in the Department of Defense. It just got renamed to the DoDIAC for architecture framework; they are thinking of leaving off the "I". There is a new version of it just out but C4ISR said if you do things in an operational view, a system view and a technology view that is what drives our specifications. The FEA on the other hand, sits above that. I believe we have not really defined a relationship between OMB and DoD, between the FEA and the C4ISR. I believe it sits above that by saying here is a business reference model, here is a performance reference model, and here is a technology reference model. Again, we may be putting too much on ourselves to do these things. I also believe you can do information modeling before DoD or Homeland Security has to make a heavy investment in their IT. So information modeling is going to keep rising, business case models, business case analysis, and most important user needs is if it counts. We need to get it right this time. We need to listen to the user and they need to listen to us on what the tradeoffs are. Web services, network-centric says many to many. It will certainly have to have interoperability as a key component of it. You get in there, find out what is going on, put your question out and you have no idea who's responding to you but you get your right information. Next slide, please.



I asked you if you knew about the future of logistics enterprise. This is part of the 2020 vision for DoD, the period of time between 2005 and 2015, and of course interoperability is the foundation for effective joint multinational and interagency operations. Interoperability is mandated for the joint force of 2020, especially in terms of communications and information sharing. That is part of the 2020 vision of DoD. The future logistics enterprise is their near-term blueprint to improve military effectiveness and logistic support through end-to-end customer service and enterprise integration based on what we call the six-pack. Total life cycle system management, acquisition and logistic support of a life cycle are now one. We are not going to have the acquisition group buy something and by the time it is acquired, turn it over to another entity. The program manager has that responsibility. Right now DoD spends about $62 billion on sustainment and there are approximately 600+ information systems that make up DoD logistics. We want to get a smaller footprint and we want to do end-to-end distribution where one person has responsibility for that distribution. We want to get to an executive agent that could be that one person for end-to-end distribution of commodities. Now condition based maintenance is all about prognostics and diagnostics and the plus is the enterprise integration to that activity. So if I have a prognostic and I find that there is a component error, I will be able to tap into the acquisition system and place my order in an automatic way. One of the biggest problems I can tell you that we have is getting DATA. We are trying to model the future and then take it to the Marines for example and say here is where you need to go, let us model where you are today and then show you the deltas by performing gap analysis. We are doing all this using the supply chain reference model SCOR because we hope the DoD will begin to act and will acquire or SCOR as a concept for supply chain management.

And my time is just about up, so I just want to say thank you very much and watch out for all those paradigm shifts, and watch out for the pig.

Iridium Satellite

"Leveraging a Global and Adaptable Infrastructure"

Mark Adams
Chief Technical Officer
Iridium Satellite LLC
September 2003

Iridium Satellite LLC Overview

The Iridium system was acquired in December, 2000, allowing the commercial service to be re-introduced in March, 2001 with a maintainable cost structure. Iridium Satellite utilizes a vertical market distribution strategy (i.e., voice and data services), and has a strategic relationship with Boeing for satellite operations and maintenance lasting through 2013.

The objective of the Iridium system is to provide a long-term stable infrastructure with global coverage of mobile voice, data, messaging, and paging services.

Iridium Capabilities- US Defense Department

Iridium provides secure, on-the-move global voice/data for the special requirements of the Department of Defense (DoD). Iridium has a dedicated, secure DoD Gateway, independent from foreign infrastructure. This allows for communications security and seamless DoD network connectivity (i.e., DISN, FTS, ILD, NIPRNET, SIPRNET). The system provides global pole-to-pole coverage (90S - 90N for Polar Regions) and allows for minimal set-up time, priority access and enhanced DoD services. There are no gaps in coverage over the ocean areas. Iridium also provides Airborne Service through a Stand Alone High Penetration Pager.

Iridium Network Performance

Voice/Data: Iridium demonstrates extremely high levels of performance both at the Tempe and the DoD Gateways. The Tempe Gateway shows a 99.2% call success rate, with only a 0.6% call drop rate (8,590 weekly test calls) for voice/data. The DoD Gateway recorded a 98.5% call success rate with a 1% call drop rate (8,407 weekly test calls). The average call duration at the DoD Gateway was nearly 6 minutes with hundreds of calls per month exceeding 100 minutes.

Short Burst Data Services: Performance measured at the Tempe Gateway showed a 99.64% first-attempt message success rate.

IRIDIUM
ONE SYSTEM, GLOBALLY.

Corporate Status
Iridium Satellite LLC Overview

- System acquired Dec 2000
- Commercial service re-introduced March 2001 with maintainable cost structure
- Vertical market distribution strategy for voice and data services
- Strategic relationship with Boeing for satellite operations and maintenance
- 2013/2014 constellation lifespan

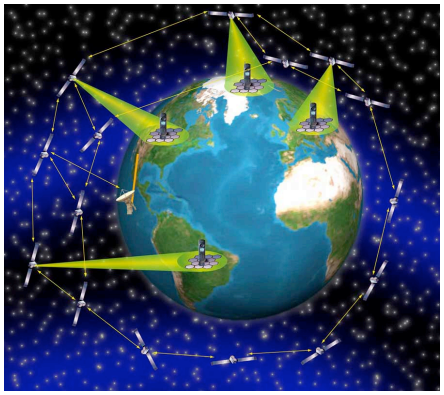
Long Term Stable Infrastructure Providing Global Coverage For Mobile Voice, Data, Messaging, and Paging Services

1

IRIDIUM
ONE SYSTEM, GLOBALLY.

US Defense Department
IRIDIUM Capabilities

Cross-Linking Satellites with DOD Gateway Provides



- **Global pole to pole coverage**
  - **Polar Regions (90°S - 90°N)**
  - **Ocean Areas (No Gaps)**
  - **Airborne Service**
- **Secure DOD gateway**
- **Independence from foreign infrastructure**
- **Communications Security**
- **Minimal Set-up time**
- **Priority Access**
- **Stand-Alone High Penetration Pager**
- **Enhanced DOD Services**
- **Seamless DOD network Connectivity**
  - **DISN, FTS, ILD, NIPRNET, SIPRNET**

Provides DOD with global connectivity via a secure DOD controlled Gateway

2

IRIDIUM
ONE SYSTEM, GLOBALLY.

Iridium Network Performance

- Voice/Data
  - Tempe Gateway measured performance: 8,590 weekly test calls
    - 99.2% Call success rate
    - 0.6% Call drop rate
  - DOD Gateway measured performance*: 8,407 weekly test calls
    - 98.5% Call success rate
    - 1% Call drop rate
    - Average call duration nearly 6 minutes with hundreds of calls per month exceeding 100 minutes
- Short Burst Data Services
  - Tempe measured performance:
    - 99.64% First attempt message success rate

* Provided by DISA

Highly Reliable, Global Secure Mobile Satellite Communication Solution

3

IRIDIUM
ONE SYSTEM, GLOBALLY.

Iridium Operational Usage

Reliability

- Command and Control
- Targeting
- Tracking

Mobility

- Deployable-on-the-move
- Pole-to-pole coverage
- DOD Priority Access

Provides secure on-the-move global voice/data for DOD's special requirements

Secure Communication

- NSA Type-1 Security
- TS Accredited

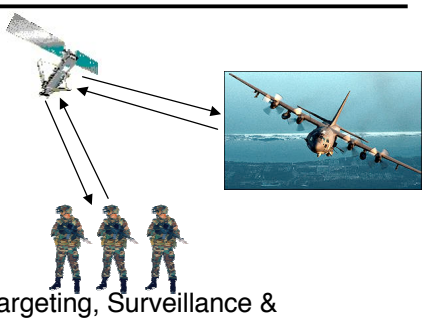
Operational Support

- Operation Enduring Freedom
- Operation Iraqi Freedom
- Homeland Security/Terrorism

4

IRIDIUM
ONE SYSTEM, GLOBALLY.

Air to Ground / Ground to Air Comm's

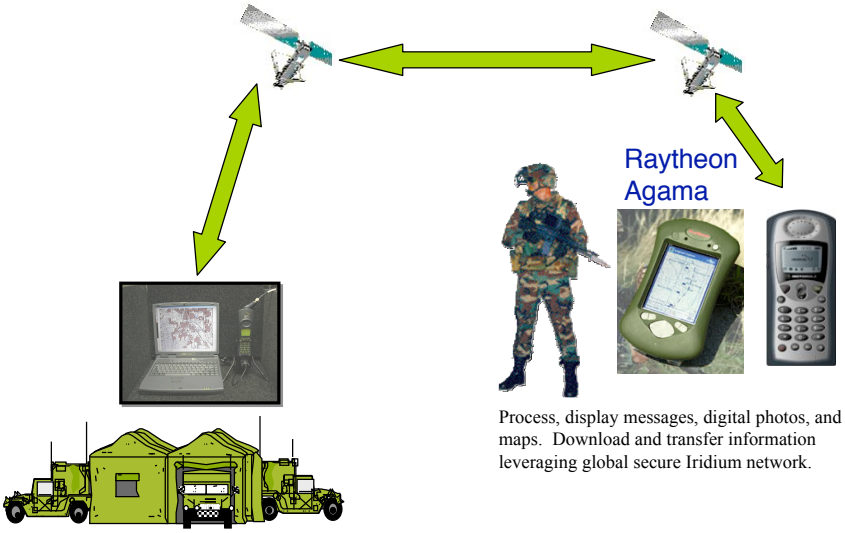


- Iridium Provides Comm's pipe
  - Over the horizon/LOS comms
  - Time Critical Targeting (Data)
  - Command and Control (Voice and Data)
  - Secure Global Reach
- Focused Situational Awareness, Targeting, Surveillance & Reconnaissance
- Worldwide Over-the-Horizon Communications using the Iridium constellation
- Common Operational Picture for the Soldier and Tactical Operations Center

5

IRIDIUM
ONE SYSTEM, GLOBALLY.

Soldier Systems



Process, display messages, digital photos, and maps. Download and transfer information leveraging global secure Iridium network.

Command Element w/Base station

6

IRIDIUM
ONE SYSTEM, GLOBALLY.

Soldier Systems

Leopard

Integrated Soldier Unit
- **Computer w/C2 Software**
- **Iridium SATCOM**
- **GPS=10 digit Grid**
- **LRF Interface=10 digit Grid**
- **Power (2 - BA5800s)**

Titan GlobeTrak

Integrated Blue Force Tracking Device

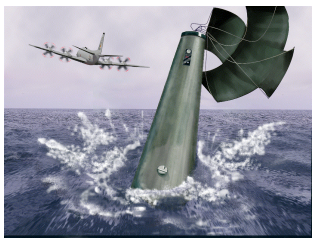
Titan's GlobeTrak Blue Force Tracking Device integrates a low-power single board computer, a global positioning system, an electronic compass, and the Iridium 24/7 global coverage into a handheld lightweight device.

7

IRIDIUM
ONE SYSTEM, GLOBALLY.

Air Craft Positioning and Reporting

- Global GPS Tracking and Messaging
- Iridium Features
  - Graphical Flight following
  - Navigation & Weather data
  - Monitors & Alerts
  - Information filters
  - Security
  - Functionality controlled at C2
  - Low - maintenance
  - Multi - platform
  - Real-time reports, messaging, positions



8

IRIDIUM
ONE SYSTEM, GLOBALLY.

Operational Usage

- **Voice services**
  - **Fixed and mobile**
  - **Clear and secure**
- **Messaging and Paging services**
  - **2-way Messaging services**
  - **1-way Paging**
  - **Broadcast alerts**
  - **Integrate pager into sensor platforms**
    - **"Wake up"**
    - **Command and control**

9

IRIDIUM
ONE SYSTEM, GLOBALLY.

Operational Usage

- **Data exfiltration applications**
  - **Fixed/mobile sensors**
    - **Photos, sensor readings, etc.**
  - **Forward observers**
    - **Command and control data**
- **Leverage Iridium data services**
  - **SBD for <2000 bytes**
    - **Low profile**
  - **Circuit-switched data for larger payloads**

10

IRIDIUM
ONE SYSTEM, GLOBALLY.

Operational Usage

- **Tracking applications**
  - **Blue Force tracking**
  - **Pallet drops**
  - **Airplanes, e.g. CAPSTONE**
  - **Mobile sensors**
- **Leverage Iridium for global reachback**
  - **SBD or circuit-switched data**
  - **GPS coordinates delivered to fixed or mobile operations center**

11

Wireless Sensor Networks

Technology for Detection and Protection

Mike Horton
President & CEO
www.xbow.com

Crossbow Background

- Founded 1995
- Venture Funded - $13M in Financing
- Shipping Sensors since 1996
- Two Major Product Lines
  - Inertial MEMS Sensors
  - Wireless Sensor Networks
- ISO9001 Certified and FAA Certified

Wireless Sensors for Security

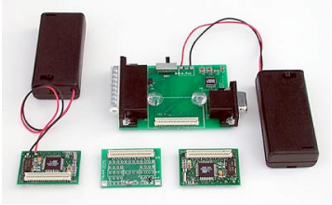
- Objective & Program History
- Deployable Scenarios
- Technology
- Current Results
- Next Steps

Program Objectives

- Tiny, cheap, air-dropped or hand-emplaced sensors that communicate detections from anywhere to anywhere in near real time
  - Perimeter area protection
  - Remote observation and search for personnel or vehicles

Program History

- 2000 – UC Berkeley develops COTS Smart-Dust Sensor (aka MICA Mote)
  - **TinyOS** Operating System created to program these sensors
  - > 3000 units delivered

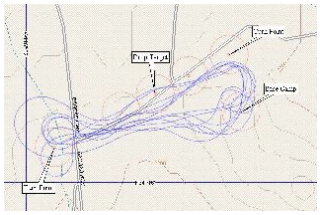


Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Program History cont'd

- March 2001 Mote + Magnetic Sensor dropped from UAV at 29 Palms



Vehicle detection successfully demonstrated
UAV / Aerial delivery demonstrated by UC Berkeley Team Using Crossbow Hardware

Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Program History cont'd

- January 2002: BALD CAMEL Project Start
  - **Commercialize** 29 Palms Capability
  - New **Improved** Sensors
  - **Longer Range** Radio
  - **Satellite Data Exfiltration**
- April 22nd 50 Mote Test at Quantico

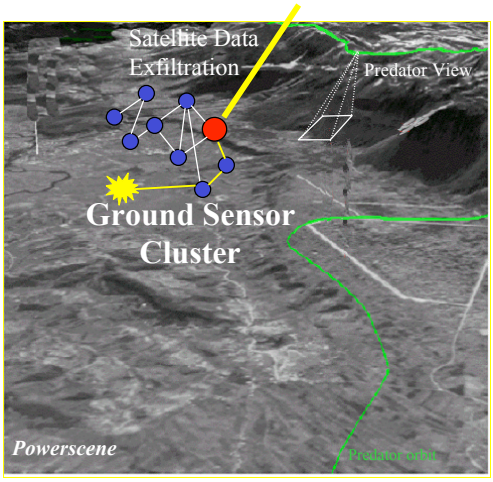
Program History

- January 2003 – MICA2 Mote & Kits
  - Increased Radio Range
  - TinyOS 1.0 Release
  - Over 300 Groups Active
  - > 20,000 Units Deployed
  - Not only military & security applications
    - Environmental Monitoring, Industrial, Building Controls, and Automotive

Scenarios

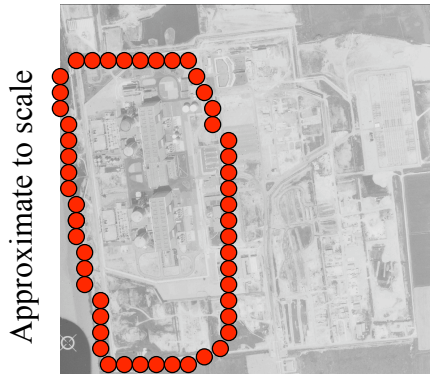
- Remote Surveillance Operations
  - Detection of people or vehicles in an area
- Nuclear Power Plant Monitoring
  - Sentry function, alert on encroachment
- Force Protection
  - Alert on encroachment, monitor previously cleared area

Remote Surveillance



- Networked Ground Sensors
  - Wide area 24/7 coverage
- Cover Personnel detected to 30m
- GPS on each sensor
- Satellite Data Exfiltration
  - Realtime response
- Sensor hit cues Predator

Power Plant Monitoring / Force Protection



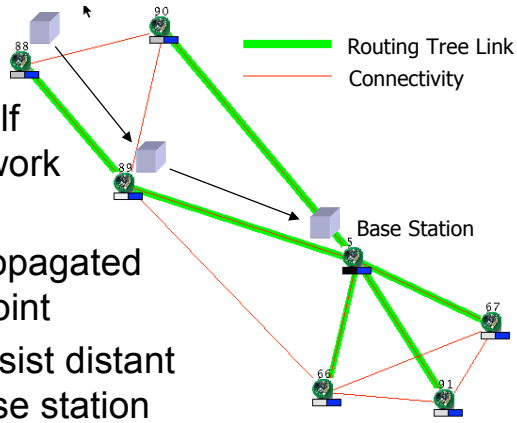
- Networked Ground Sensors
  - Wide area 24/7 coverage
- 50 sensors can cover physical area of plant
- Rapidly deployed to threat
- Sensor hit cues security action

Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Technology: Ad hoc sensing

- Autonomous nodes self assembling into a network of sensors
- Sensor information propagated to central collection point
- Intermediate nodes assist distant nodes to reach the base station



Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Technology: Radio Link

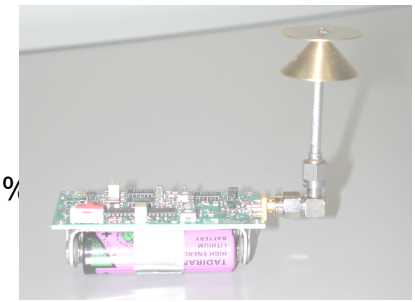
Radio Modulation	FSK, Frequency Hopping (optional), 433MHz, 900-928MHz
Range on Ground (ft)	100-250
Range above Ground (ft)	500-1000
Max Power (mW)	10
Sleep Current (uA)	5
Transmit Current (mA)	20

Technology: Sensors

- Mote architecture versatile supports any analog or digital sensors
- Current sensors and detection radius:
  - Magnetic — Vehicles at 20 ft radius
  - Seismic — minimal range < 5 feet radius
  - Acoustic — discrimination possible, complex
  - ➢Radar — 50 feet radius, vehicle & personnel

Technology: Ultra Wide Band Radar

- Developed at Lawrence Livermore
  - Advantaca spin-out
- Low-power
  - 6-10 days on 2X Li AA @ 100% On
- Small form factor
- 50 ft Detection Radius (hemisphere/bubble)

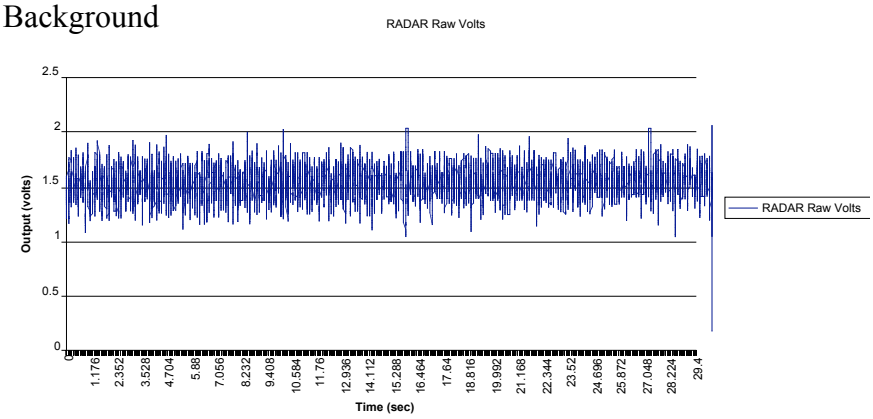


Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Technology: UWB Radar

Background

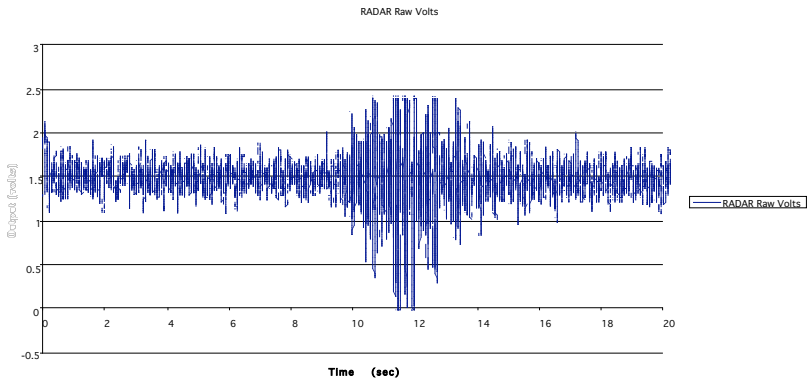


Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Technology: UWB Radar

Human Walk Thru at 50 Feet

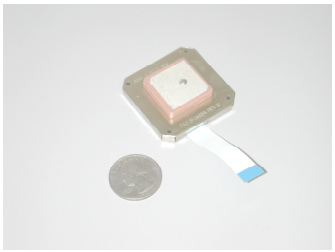


Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Technology: GPS

- Small low-power GPS module
- Standard 12-channel L1 Module
- Location service at power up
- Optional synchronization service for low-power ops



Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

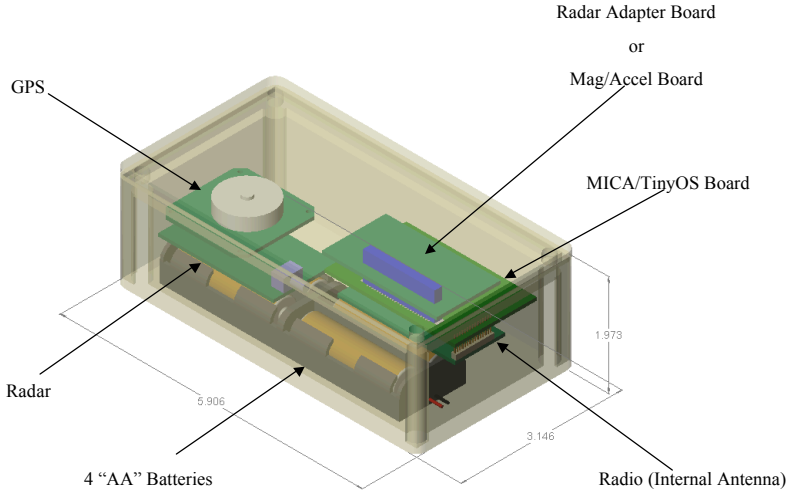
Technology: TinyOS

- Tiny OS
  - Detection Networking built on top of TinyOS 1.0 (http://today.cs.berkeley.edu/tos/)
  - Detection algorithm radar – envelope detection with near field event rejection
  - Magnetic anomaly detection algorithm
  - GPS Power control
  - Satellite Link control
  - Hearbeat radio messages

Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Integrated MSTAR Mote



Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

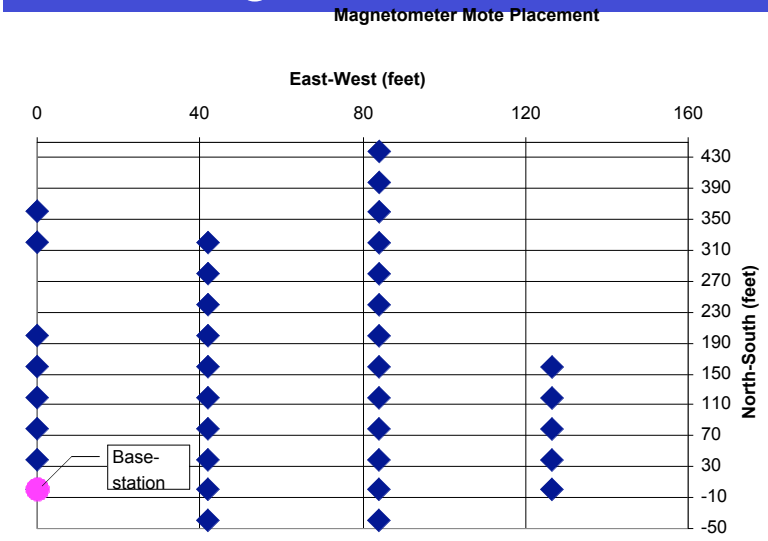
Base Station Software

- Overlay satellite image
- GPS Coordinate display
- Detection status, history

Results

- Magnetic Array Test
- Drop Survival Test
- Radar Array Test

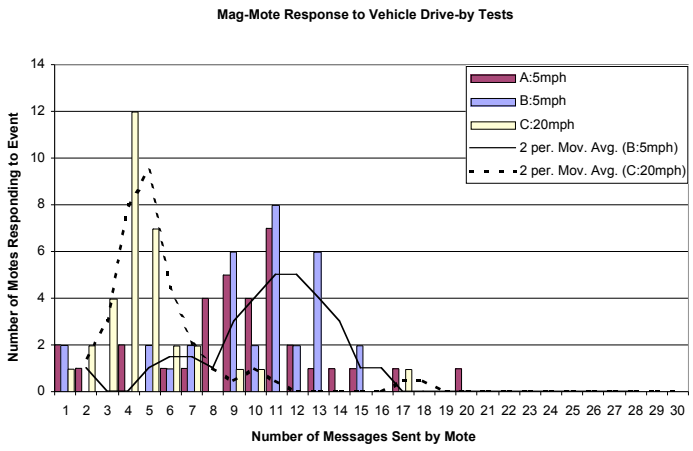
Magnetometer Grid



Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

Magnetometer Test



Crossbow
Smarter Sensors in Silicon

Developing the New Infostructure

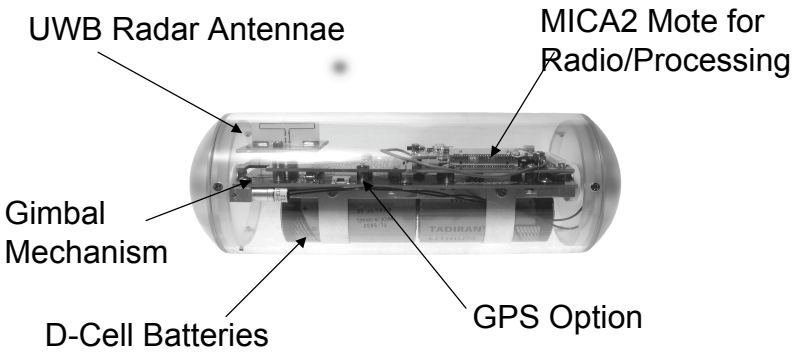
Drop Survival Test

- 400 ft drop
- Initial survival
- 3 week Environment test

Radar Array Test

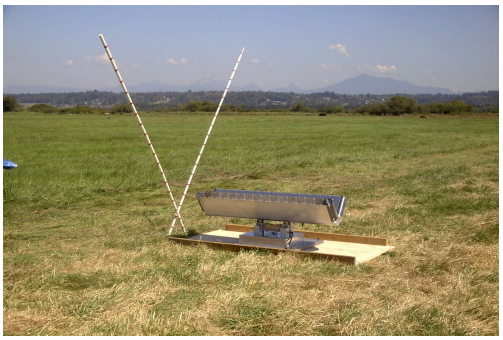
- Preliminary Test Completed
- 6 Units, Flat Terrain
- Slow Movement Detection > 90%
- Low False Detections
- Issues:
  - Array Pattern Control
  - Landing Orientation

New “Self-Righting” Package



Packaging designed by Advantacca

Dispenser Testing



- Ground Test
- Upside Down mounted to Bomb Rack
- 30 Sensors
- 1 sec intervals

Testing and dispenser completed by Systima Technologies

Next Development Steps

- Complete Iridium Satellite Link Mote
- Additional sensor work
  - Radiation sensor
  - Acoustic and Video capture
- **Test and deployment**

Wireless Sensor Networks

Technology for Detection and Protection

Mike Horton
President & CEO
www.xbow.com

An Information-Centric Approach to the Global Information Grid

Thomas McVittie, PhD
Chief Software Architect – Deep Space Mission Systems
Jet Propulsion Laboratory
California Institute of Technology
Email: mcvittie@jpl.nasa.gov

Abstract

The Global Information Grid promises to greatly enhance our ability to effectively locate, compose/combine, collaborate and distribute information on an unparalleled scale. We believe that an information-centric architecture comprised of powerful interoperable information models and a simple set of ubiquitous generic services is essential to enabling the GIG vision to rapidly become a reality. During the past six years, we have employed these techniques to create and deploy information-centric services in a number of operational contexts. This paper presents an overview of the information-centric approach, its applicability to the GIG architecture, a brief survey of two current information-centric systems (one at the tactical level and the other at the JTF), and outlines future research and experimentation.

1. The Decision-Making Environment

Today's operational environment is becoming increasingly complex. Force and Intelligence assets are normally multi-lateral and composed of elements from coalition, NATO, and several US services and agencies. These elements and their commands are often involved in multiple simultaneous operations, which may overlap in unexpected ways exposing conflicting goals and contention for limited resources (e.g., humanitarian assistance vice force protection.) While many of the fundamental decision-making processes have not changed, the speed at which they need to occur is becoming much shorter and the shear volume of data that needs to be taken into account is becoming much larger.

Figure 1 is reasonably representative of a typical real world situation involving multiple elements collaborating to solve a dynamic problem. The Marine Reconnaissance, Surveillance, and Target Acquisition (RSTA) team has identified a vehicle as being a threat and requests fire support from a sister agency (USA). The USA selects appropriate munitions and the weapons effects system calculates the resulting fire effects fan. One or more Geographic Information Systems (GIS), or more likely a human, identifies resources (roads, buildings, people, etc.) that may be impacted based on the overlap between their reported locations and the probable effects fan. Another system, or human, evaluates these impacted resources based on information available from national/regional sources (such as MIDB and HUMINT) to determine whether the proposed action or side effect is in compliance with the commander's intent. The commander takes input from all of these sources, combines it with his/her judgment and doctrine, and determines whether or not to execute the fire mission.

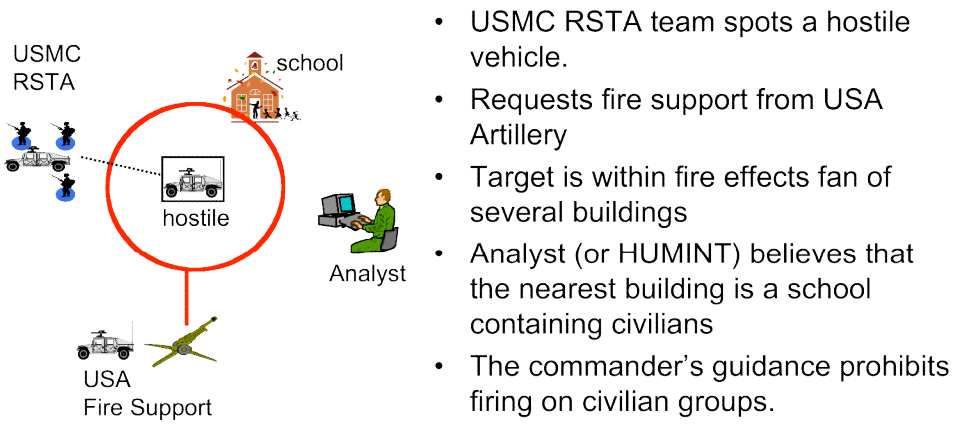


Figure 1: Real world situations are collaborative and dynamic

While we used a fire mission as the example, this same type of activity occurs across a wide variety of situations – each of which shares a common set of characteristics:

- They involve collaboration across multiple discipline-specific teams/systems each having a particular mindset and understanding of only a subset of the whole situation. For example, the fire team may not know why the Marines believe that the target is hostile; the Marines may not understand the fire effects fan associated with the Army's choice of munitions; and the GIS only understands the world in terms of spatial relationships.

- There is a need to build and communicate a common understanding of the situation and its ramifications based on the contributions of people/systems representing multiple sources and information domains. Not everyone (or every system) needs to share the same viewpoint or data, but where their data/information needs overlap there must be a clear and unambiguous understanding of what the information means.

- They are dynamic – changes in information from one person/system can have a significant impact on the overall decision. For example, what if a coalition HUMINT source asserts that the school contains a terrorist cell rather than a group of civilians?

Supporting this type of situational-awareness and decision-making, particularly in the presence of increasingly capable communications systems, and the much richer data feeds available from the Global Information Grid (GIG), will require significant changes to how we build computer systems, and how we expect users and computers to communicate.

Over the past six years, we have been collaboratively building computer systems using an information-centric approach, which specifically addresses this need. We have fielded these systems in a number of different environments (tactical, JTF, etc.) and in support of various US services. We believe that these approaches are compatible with, and essential to the support, of the emerging Global Information Grid.

The remainder of this paper is organized as follows. Section 2 discusses current DoD approaches to integrating data/information feeds from multiple sources. Section 3 provides an overview of the information-centric approach and its benefits. Section 4 examines two systems that have been built based on the information-centric approach. Section 5 compares this architecture to the needs of the GIG and proposes areas of collaboration. Section 6 presents conclusions.

2. Building Situational Awareness

As mentioned previously, real world decision makers usually require information from several sources and multiple information domains in order to understand the situation in context. Unfortunately, the way we traditionally develop systems results in a set of applications that are designed to provide a specific set of capabilities to a particular set of users (e.g., Field Artillery Fire Support or Army Tactical Maneuvers). As a result, these systems often represent data in their own formats and make only a small subset of their capabilities available through application unique APIs and protocols. While this is not a significant problem for the applications themselves, it makes the process of combining data from multiple (independent) sources much more difficult.

2.1 Standardized Messages and Hubs

As shown in Figure 2, one widely used approach to integrating data from multiple systems is to develop a standardized message set or translation hub to exchange critical data between particular systems.

While this approach has been somewhat successful, it has a number of limitations:

- Only the most critical aspects of data are exchanged. The majority of information maintained by the systems is NOT available to other systems.

.

- The approach tends to be fragile especially if the message formats need to evolve over time to support new types of information or concepts. Trying to coordinate the evolution of these interfaces across a large number of systems is a very daunting task.

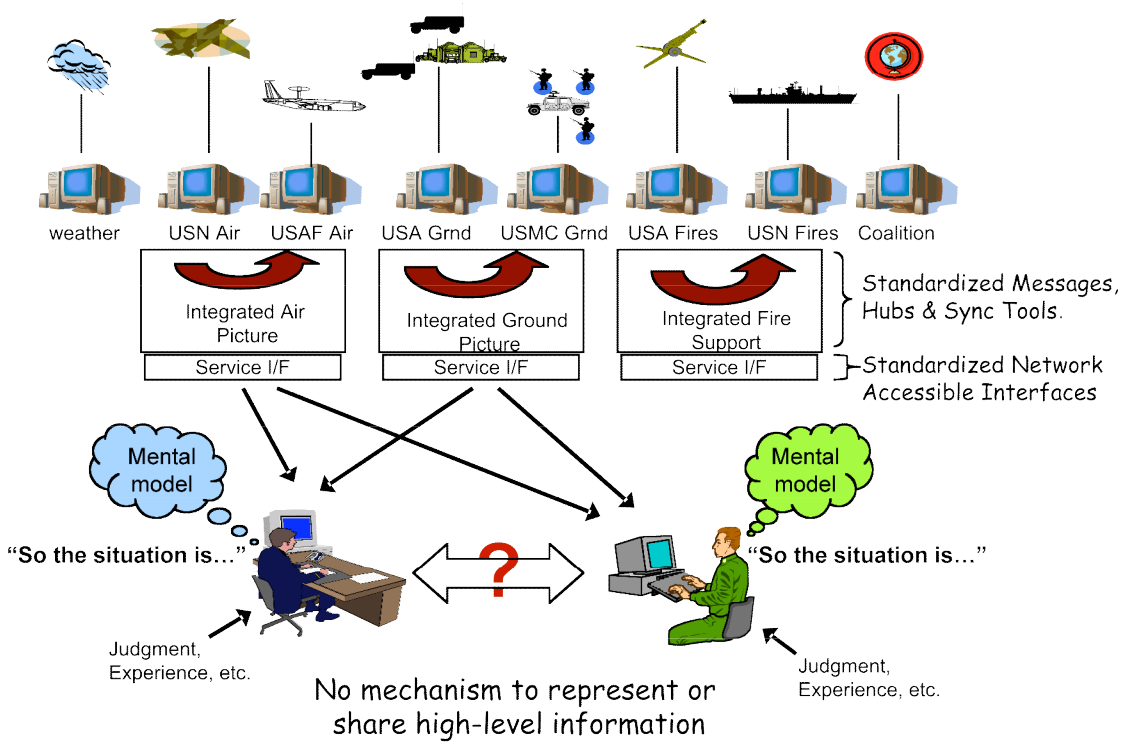


Figure 2: Building situational awareness

- The interfaces provided by the various systems are often well defined in terms of syntax, but poorly defined in terms of semantics – we know the format of the data, but have a much less certain understanding of what it means.

- Most of the efforts are focused within a very narrow information domain (e.g., integrated air picture) and are focused on tying similar systems together. There are very few examples where information/data is shared across domains. In effect, we tend to merely create larger domain-specific stovepipe systems.

2.2 Services Architectures

More recently, industry and DoD have embarked on an effort to use a service-oriented approach to making data/information services available across the network. This approach advocates replacing application-specific APIs and protocols with a common set of industry-standard protocols (e.g., SOAP) and data packaging formats (e.g., XML schema). For example, a messaging hub wrapped in a services interface is often referred to as a "Mediation Service".

While this approach will improve our ability to readily access the capabilities of different applications, it does little to address the content of the information and virtually nothing to allow

us to combine information from multiple sources. In effect, the Mediation Service suffers from the same limitations as their message hub predecessors. We should view service-architectures as merely a technique for providing simpler standardized mechanisms for accessing capabilities across the network -- not as a quantum leap in our ability to provide and share situational awareness.

2.3 Sharing the Big Picture

Perhaps the most significant limitation of our current approach is that *it does not support the human decision-making process*. Returning to Figure 2, each user receives data from multiple systems and, based on their own experience and judgment, creates a "mental model" which they then use to reason about the situation. This mental model is usually quite rich and composed of key objects (say RSTA teams, buildings, hostile targets, fire teams, etc.) having a reasonably well-understood set of capabilities and behaviors (e.g., we do not expect buildings to attack, nor do we expect RSTA teams to contain civilians). Each user augments the mental model using a rich set of relationships between the objects (e.g., the Fire Support team is engaging the hostile target, the building is a school which MAY contain civilians, etc.)

This type of "mental modeling" is very powerful and provides humans with the ability to efficiently reason about extremely complex situations. *Unfortunately, our current systems can only maintain/distribute their domain-specific data. They have no means to maintain or communicate the user's mental model (and its linkages to the underlying data) to another user.* Users are forced to use "out-of-band" mechanisms, such as text messages and voice, to communicate their mental model – and the person receiving the communication must manually reconstruct the mental model based on the contents of the voice/text messages. Unfortunately this approach does not scale to more than a few collaborations, and the linkages between the mental model and the underlying data are usually lost.

If we are to make any significant advances in sharing information and our mental models, we must fundamentally change the way we think about building systems. Specifically, we need systems that:

- Represent information and concepts in real-world terms that are understandable by both humans and machines (software agents). We need to bring systems up to our level, not continue to require humans to read machine-convenient formats and representations.

- Are natively able to span multiple information domains. Integration of information from multiple domains and sources should be our driving focus, not an afterthought.

- Can readily augment our existing data/capability-based systems by coordinating their activities and information flows. We need the ability to orchestrate the systems that we already have so that they can collectively better provide the capabilities we need.

- Are "open" – there should be no significant barriers to accessing data/information or adding new capabilities. We need to change our viewpoint from "… my data that I'm willing to share with some of you" to "… our information".

We have had the ability to build this type of "information-centric" system for a number of years. In our experience, they are relatively straight forward to develop and provide a significant improvement in not only our ability to share information, but also in providing a reusable open platform for easily adding additional information producers/consumers and even decision-support agents. In the following sections we will explore the basic concepts of an information-centric architecture, and examine two current implementations.

3. Information-Centric Architectures

Not surprisingly, an information-centric approach begins by determining the information and concepts that need to be maintained and exchanged in order to support specific decision-making communities. As such, an information-centric system intended to meet the needs of a fire-support coordination community may require deep knowledge of the fire control process, weapons effects, and less detailed knowledge of logistics/resupply, and commander's intent. While an information-centric system intended to address a battlefield planning and shaping community may need a broader, and potentially less deep, knowledge of maneuvers, weather, enemy order of battle, and fire support.

Once the concepts and information have been identified, the information-centric approach creates an information model that is familiar to humans and can be readily understood by computers/agents. The resulting information model is then wrapped with a generic set of network accessible services that allow new and existing systems and humans to efficiently interact with the information services and with each other.

This last point is significant. The same software approaches can be used to provide a low level track data service, a higher-level C2 situational awareness (information) service, or a cross-domain readiness service. The information model determines how the system functions and what capabilities it will have. This provides an unparalleled level of flexibility in tailoring systems to meet the needs of various communities and users.

In the following subsections, we will take a more in-depth look at the two primary components of the information-centric approach: the information model; and, the generic information services.

3.1 Information Models

Information models are the heart of the information-centric approach. The extent to which the information model is able to represent complex real world concepts and information in a manner that is not only familiar to human decision makers, but also suitable for automated processing

and agent-based decision-support systems will determine the effectiveness of the information-centric capability as a whole.

In the information-centric approach, information models are comprised of the three distinct tiers shown in Figure 3.

- **Data dictionaries** provide for a consistent understanding of terms within an information domain (community). As such, they contain at a minimum: precise definitions; validation criteria; default values; and, constraints.

- **Object Models** provide the fundamental basis for information exchange by defining the logical structure of information in terms of objects that are created from collections of data dictionary elements. These objects may represent real world objects and concepts or even agreed upon interfaces and messages. As such, the primary focus is on schemas, structures, and object behaviors.

- **Ontologies** can be thought of as providing special purpose "mental" models tailored for specific decision-making needs. They are created from entities in the object model layer augmented with rich inter-object relationships.

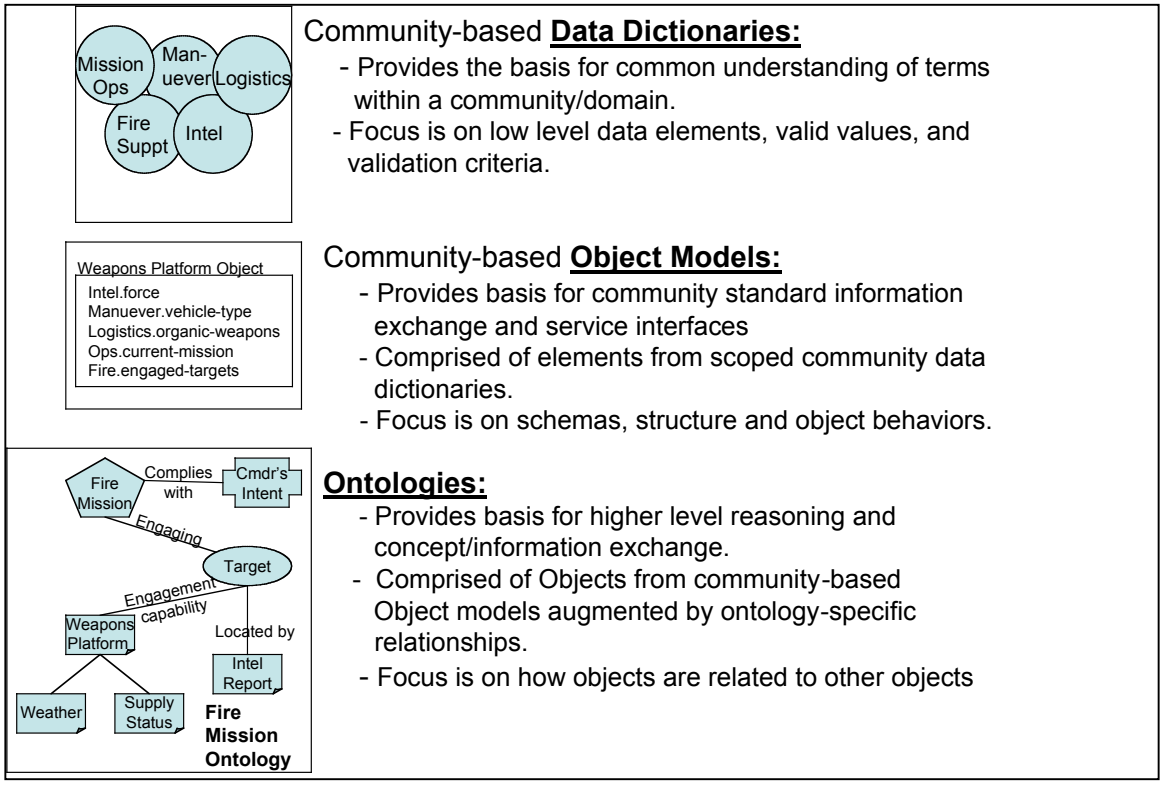


Figure 3: Information tiers

While each of these tiers is useful, it is their interaction that powers the information-centric approach. Domain-specific data dictionaries provide a consistent and unambiguous taxonomy of a particular subject matter - thus avoiding "semantic mismatches" where the meaning of an element is not fully shared between two parties. By requiring that object models be constructed exclusively from a common set of domain-specific data dictionaries, we provide a consistent basis for mediation between various objects without requiring all systems to use the same object model. Through the creation of ontologies by augmenting object models we allow the ontology to not only span multiple systems and information domains, but also provide the basis for different purpose ontologies to collaborate (say a logistics ontology and a tactical operations ontology) through either common objects or common elements in the object model and data dictionary tiers.

It is important to note that we expect any given community to use several different ontologies (each for a particular purpose), which may be comprised of different subsets of the various community object models and data dictionaries.

By intent, the tiered approach focuses the most rigor and required uniformity on the data dictionary level where it is also most likely to be successful due to the narrow domain focus (i.e., it is easier for a group to agree on the meaning of "air speed" rather than on what makes up the concept of a "fire mission"). It also provides the most flexibility at the ontology tier where we expect that the representational needs of the various decision-making systems (and their human users) will vary greatly.

3.2 Generic Information Services

An advantage of the information-centric approach is that the complexity of the system rests primarily in the information model(s). The services supporting the model and its interactions with users/systems are usually quite simple and to a large extent can be automatically generated from an abstract representation of the information model (say UMI). For example, an information-centric system intended to aid in the search and retrieval of text documents[1] would be based on a document information model such as the Dublin Core. While a system intended for tactical C2/Fires interoperability would be implemented with an information model supporting very different concepts. The same basic set of software services can be used to provide both capabilities.

[1] In cases where the resulting information model closely parallels one provided by industry, it may be productive to look for COTS solutions.

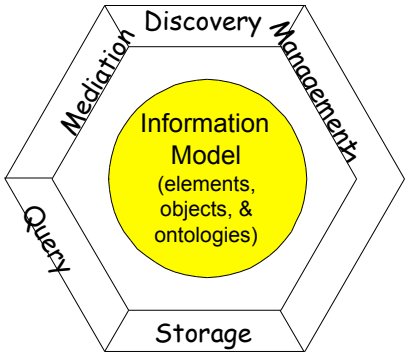


Figure 4: Information-centric generic services

As shown in Figure 4, there are six core services each that are customized to various extents to support the underlying information model. These services include:

- **Storage** – responsible for maintaining and persisting instances of the information model.

- **Query** – allows users/systems to search through instances of the information model for information and relationships of interest. Information can be returned either synchronously or asynchronously.

- **Mediation** – serves as the primary interface between this information-centric system and any other systems (either information or data centric). Typically mediation services are heavily customized to support interaction between existing data-centric systems and the other information-centric services. For example, as discussed in the next section, a mediation service may act as a client (or peer) of an existing system and bi-directionally translate between the information model and the other system's public message formats. It is important to note that data systems are mediated through the information model, not directly to each other. This minimizes the complexity of the mediation service and ensures that we correctly map the concepts (semantics) as well as the syntax of the existing systems. It is not unusual for multiple different mediators to exist in a single deployment.

- **Management -** provides the ability for information model aware components to add, delete, clone and modify objects and manage their associations and relationships. The structure of the management service interface is generated directly from the UMI model which, along with the data dictionary, contains sufficient information to provide basic entry validation and enforcement of required (vice optional) attribution and association.

- **Distribution/Synchronization** – notifies interested parties (via a configurable set of network protocols) of changes to the instances of the information model. This

service supports a prioritization scheme that allows user-perceived critical information to gain precedence when communication resources are limited. The same service is used to not only distribute information to clients, but also to maintain a tailored (information-based) synchronization between cooperating information-centric storage servers. Since the various components "share" the information model, only the changes need to be distributed and only to those who are interested. These approaches result in a significant reduction in bandwidth needed to synchronize servers and to distribute information to clients.

- **Discovery** - provides a mechanism for information-centric servers to describe the information they manage and make available. This is primarily used to determine not only which servers can provide a given set of information, but also the form of the interfaces.

Figure 4 is intended to stress that each of these generic services relies on and supports the information model. However, Figure 4 should not be used to imply that the services are co-located or that the information model must be monolithic. In fact, these services are generally distributed across the network and are either replicated or directly incorporated into other applications. For example, in highly disconnected networks, clients or applications can use local instances of the storage, query, management and distribution services to act as local information caches. These clients and applications are unaware of whether they are using their local services or the main services – it is up to the distribution service to adequately synchronize the instances. Likewise, multiple mediation services may be instantiated acting as either mediation hubs (supporting multiple existing systems) or single system mediators.

This generic approach has also enabled the service implementations to undergo significant evolution/adaptation without requiring changes to the other services or systems. For example, the first instances of the management and distribution services were built on CORBA and the storage service was built on the Object Store object-oriented database. However, as the system was fielded over increasingly limited communications infrastructure, the overhead of CORBA became unattractive. Additionally, as we fielded more instances, the licensing costs associated with Object Store became prohibitive. As a result, the management and distribution services were converted to a set of simple Java services, and the storage service was modified to use 'mySQL' - a relatively simple relational database. This type of flexibility will be essential in not only supporting the wide variety of deployment environments, but in evolving our approaches to meet service and GIG-wide infrastructure services and tools requirements.

3.3 Advantages of the Information-Centric Approach

There are a number of advantages of the information-centric approach:

- Systems are built around the information and concepts that need to be shared. As such, interoperability and collaboration are designed into the system from the start, not added as an after thought.

- Concepts and information are represented in a form that is familiar to humans and understandable by machines allowing both humans and agents to understand the context and be able to reason about the situation. This is in sharp contrast to current approaches, which tend to focus on machine representations requiring humans to understand and adapt to these formats.

- Many of the detailed tasks associated with monitoring data can be delegated to agents. This approach is essential if we are to be able to handle the vast amounts of data that the GIG will make available without hiring an equally vast pool of human analysts.

- The complexity of the system is in the information model, and much of the software can be automatically generated. This allows significant portions of the software developed to support one information-model to be reused to serve a different information model.

- The focus on network accessible generic services breaks down the traditional vendor boundaries – any organization is able to deliver capabilities that either provide or consume parts of the information model. This can encourage a best-of-breed environment.

- The approach provides an environment that readily supports existing data-centric systems. Not only can these systems continue to operate, but they can often benefit from a richer source of data (e.g., a fire control system could effectively receive blue position reports from any available source without needing knowledge of how to interface with those particular systems.) Again, we want to coordinate the existing systems, not replace them.

3.4 Bridging Existing Data-Centric and Information-Centric Systems.

While it is clear that information-centric systems show great promise for enabling us to maintain and share concepts in new and powerful ways, it is equally clear that we have a significant investment in our existing data-centric systems. Moreover, many of these systems currently have deep subject-matter knowledge that, while not publicly exposed in a reusable manner, allows them to provide essential services. Rather than choosing between data-centric and information-centric approaches, we need to adopt an approach that allows the two approaches to augment each other.

One common approach is to use an information-centric architecture to represent higher-level concepts and orchestrate collaboration between existing (and often non-communicating) data-centric systems. The information-centric system orchestrates the collaboration by using the mediation service to interact with each of the existing systems and translate activities at their public interfaces (including event channels, messages and database triggers) into appropriate changes in the relevant portion of the information model. Similarly, the mediation and distribution services are used to distribute changes in the information model to the existing

effected systems again using their public interfaces. In effect, each system contributes and consumes part of the larger conceptual "picture" maintained by the information-centric system. In addition, the information-centric system provides a new and powerful platform for adding new capabilities. Agents or applications can be created that can directly use the information-model freeing them from detailed knowledge of the system producing the information and its particular format and access mechanism. For example, a developer creating a Blue-on-Blue agent to monitor and avoid fratricide could directly use the information model's representation of units, firing fans, and fire missions to determine that a fire mission might result in friendly casualties. The information-centric system would automatically deal with the nuances of interacting with the existing systems reporting various friendly (blue) positions, systems reporting weapons solutions, and fire effects databases.

4. Current Information-Centric Systems

During the past six years, a group[2] representing government, industry, and academia have been collaboratively developing and experimentally fielding systems based on the information-centric approach for various DoD organizations[3]. While the capabilities and fielding environment have varied dramatically, the high level architecture and services have remained virtually identical.

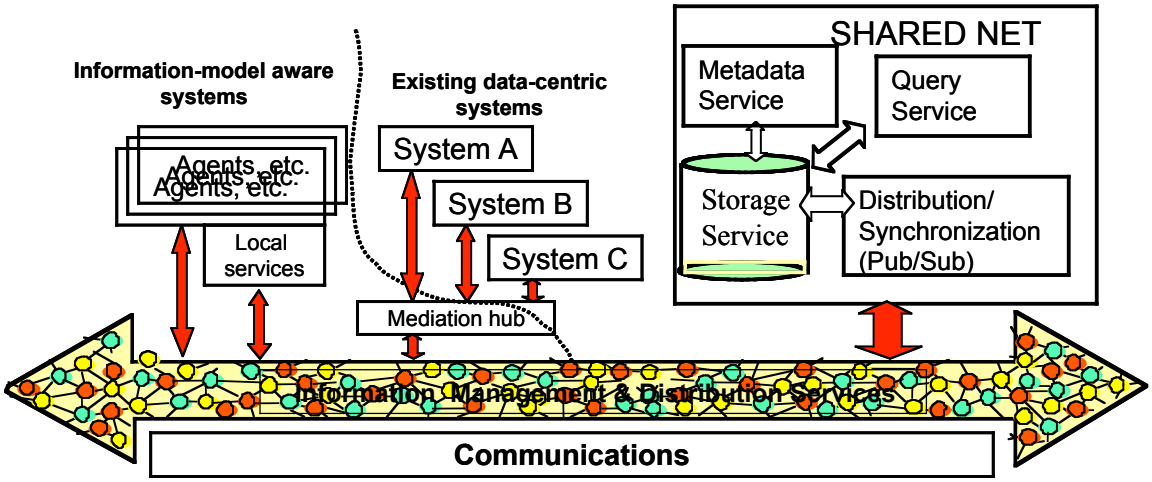


Figure 5: Generic system architecture

Figure 5 provides a high level conceptual view of our implementation of an information-centric architecture. The information model (shown as a web of circles) is served by the generic set of information services discussed earlier. These services can be distributed on the network or centrally hosted. Existing data-centric systems (which represent the bulk of the systems in most of our fielding) use the services of one or more mediators to integrate with the information model

[2] Collaborators include: Government: SPAWAR SSC, JPL/NASA, & NRL Stennis. Industry: FGM Inc., CDM Technologies, and SRI International. Academia: Cal Poly San Luis Obispo and Cal Tech.
[3] Sponsoring agencies include: Marine Corps Warfighting Lab, Office of Naval Research, Extending the Littoral Battlefield ACTD, JTF Warnet, and DARPA.

maintained by the storage service. The mediator (itself an information-model aware system) interacts with the other generic services to service the needs of the existing data-centric systems. Other information-model aware capabilities such as agents, client visualization and decision-support tools interact either with the main or local instances of the generic services.

In order to better understand the architecture, we will look at two different systems built using the same approach and generic services, but using widely different information models. In both cases, the Shared Net and Translator software are co-hosted on a Pentium III laptop with a standard memory configuration.

5.1 The C2 Translation Database (C2TD)

As shown in Figure 6, C2TD supports collaboration between the Component-specific tactical C2 systems in a Joint Task Force (JTF) context. Each of the military services continues to use its native set of applications and tools. The information-centric system (shown as Mediation, and Shared Net – encompassing Management, Distribution, Query, and Storage) supports a JTF information-model. The model was constructed in response to the warfighter's critical information exchange requirements previously developed during a series of PACOM sponsored warfighter conferences.

C2TD facilitates near real-time collaborative planning and directly enables information sharing at the tactical level. This information sharing includes both Common Tactical Picture (CTP) and support fires data, and as it continues to develop, will include interfaces for Coalition forces operating within the JTF.

In effect, the information-centric system augments the existing systems by coordinating information exchange between the local service-specific systems (e.g., ensuring that NAVFOR's AFATDS and GCCS-M share a common blue PLI picture) in near real-time, and also for coordinating information movement between the various members of the JTF (e.g., between MARFOR and AFFOR.) The SN Synchronization/Distribution Service allows each system to subscribe to the types of information that it needs. As new /modified information meeting the subscription becomes available, the Mediation Service translates it into a format/protocol understood by the existing application. Using this approach the SN Synchronization/Distribution Service is able to co-exist with other application-specific synchronization systems - such as the COP Sync Tool (CST) or the Force Over The Horizon Coordinator (FOTC).

The various Shared Net (SN) nodes were widely distributed and connected through a variety of wired and wireless networks. Redundant SN nodes and network paths were used to avoid single points of failure.

The approach has proved quite capable during the initial LTAs and was even able to provide a relevant blue PLI picture to Link-16 equipped aircraft. Further PACOM-sponsored JTF exercises are planned within the next few months and, under the direction of OSD DUSD (AS&C) a transition plan has been developed and funded.

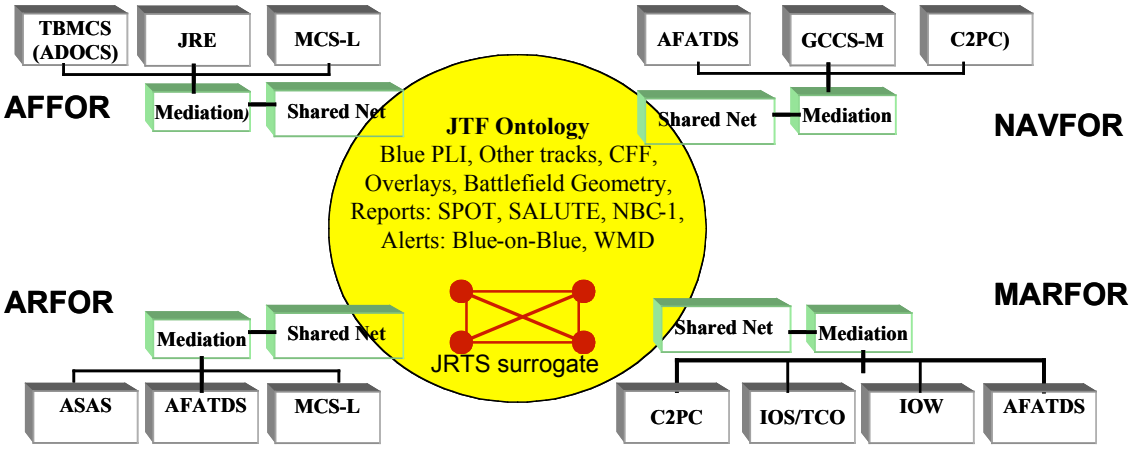


Figure 6: C2TD in JTF Warnet

Short-term efforts will focus on integrating the existing information-centric services with additional mediation tools. This will greatly increase the number of systems that can be coordinated within the JTF and promises to provide a controlled collaboration path to our coalition partners.

5.2 Integrated Marine Multi-Agent Command and Control System

The Integrated Marine Multi-Agent Command and Control System (IMMACCS) focuses on the information needed to support Marine Corps tactical operations (RSTA, STOM, etc.) and tactical information exchange with peer organizations within the USA and USN (say exchange of blue PLI or SPOT reports). As such, it has a much richer (and deeper) information-model than the one used for the JTF.

Like the JTF deployment, IMMACCS coordinates information flows between a number of service-specific existing systems. This approach greatly increases the consistency of the tactical picture at all echelons. However, IMMACCS also enriches the warfighter's existing systems by providing a set of new information-centric components that focus on enhanced visualization (users are able to follow the associations and relationships in the model – i.e., click on a fire fan and see all of the information related to the fire mission, etc.), agent-based decision support tools (including mentor agents associated with each fielded user and Blue-on-Blue agents), and an integrated Geographic Information System (lines, points and polygons on the map are related to actual objects which have behavior – i.e., the agents can reason about a route in terms of the capabilities of the roads and bridges). Both the existing data-centric and new information-centric systems are coordinated through IMMACCS and share a view of the battlespace. This approach allows each service/deployment to determine the appropriate mix of existing and new technology that will best meet their tactical needs.

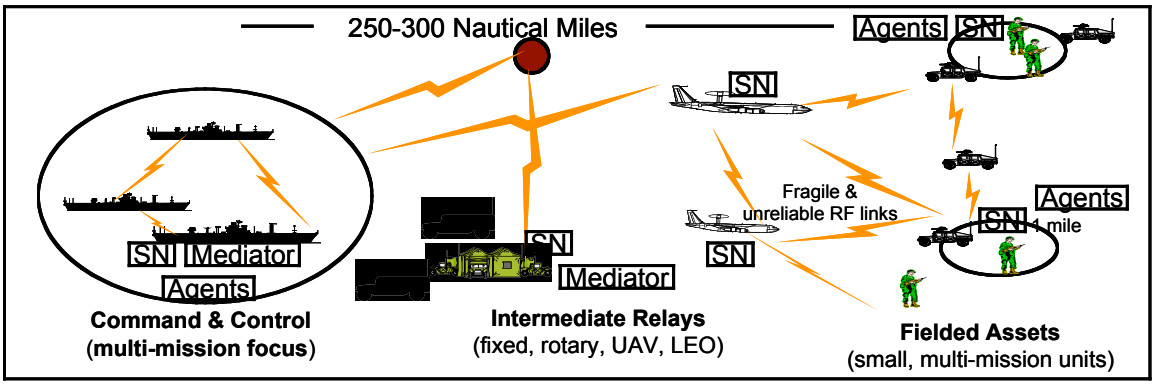


Figure 7: Tactical deployment in Capable Warrior (KBX) and ELB ACTD

As a tactical level system, Shared Net must efficiently exchange information over existing challenging tactical networks[4] where bandwidth is often extremely low (as low as 300 kps) and connectivity of assets on the move is infrequent and spurious. By co-locating the information-centric servers (shown as Shared Net or SN) with each communication node, critical information is propagated through the network (based on user/system subscription and assigned priority) as network connections are available. Essentially, each communication node becomes a fully capable proxy for the audience-relevant portions of the system as a whole. Mediators and agents are also scattered throughout the battlespace and placed where they can do the most good (e.g., Mentor agents are hosted on the user's computer, whereas mediators are hosted near the information/data providers that they mediate.)

The IMMACCS Object Model also contains the concept of a history, which allows SN to act as an archive capable of replaying any set of past events. This capability has proved to be extremely useful in not only allowing the commander to replay significant events, but also in allowing the agents and users to train using "previously recorded data" (fed by SN to the existing systems) while still being reactive to the changes they are making. In several cases, IMMACCS was even used to aid existing systems in recovering from major system failures by quickly replaying the past hour's events and thus populating their data stores with the most up-to-date information.

IMMACCS has been used as the primary information system supporting a variety of experiments and ACTDs including: Urban Warrior, Capable Warrior, and the ELB ACTD. It continues to be developed by the Marine Corps and is slated to support the upcoming Sea Viking exercises.

5. Information-Centricity and the GIG Vision.

The Global Information Grid is an extremely ambitious effort, which promises to greatly enhance our ability to share information on a truly global scale. While still in its initial phases, it is clear that there are significant similarities and synergy between the information-centric

[4] Currently supported networks include SINCGARS, EPLARS, VRC-99, Ku, and Iridium.

approach that we have been using during the past six years, and the vision of the GIG implementers. Such areas of similarity include:

- A focus on community/domain data dictionaries and, to a lesser extent, object models.

- Use of the same set of six generic services.

- Intent to provide ready access to information regardless of source.

In many ways, the differences between the two approaches are more related to the scope of their responsibilities and the extent to which they must scale than to their conceptual approaches. For example, while the GIG is responsible for understanding and fielding generic mediation services, our work has been focused primarily on C2 mediation in various operational contexts. In many ways, our experiences with information-centric architectures can be viewed as not only a strong endorsement of the GIG approach, but also a series of lessons learned and prototypes that are currently available to showcase the concepts and provide operational utility.

There are several areas of potential collaboration:

1) At the present time the DoD XML registry is the primary mechanism for developing and promoting information models. It currently focuses on the data dictionary and, to a more limited extent, object model tiers. The area of ontologies remains largely unexplored. Additionally, the process of by which a community reaches consensus on a common set of elements and objects remains unclear. The ontologies, object models, and data dictionaries developed for JTF Warnet (Joint Forces Coordination), IMMACCS (Tactical Operations), and SEAWAY (Seabasing Logistics) were developed with the operational communities, have shown their ability to interact with critical existing systems, and have been fielded in a number of operational venues. It is our belief that these existing information models could provide a significant step forward in information sharing in these critical areas.

2) The generic services, and their information-model specific instances, developed as part of these efforts are in-line with the emerging GIG architecture and can be used to provide immediate GIG capabilities to operational forces. DoD has made a significant investment in providing an information-centric system capable of mediating between several of our key maneuver and fires systems. The core information services are "open", which enables any vendor to collaboratively contribute capabilities. A particularly attractive option would be to sponsor an interoperability ACTD where contractors/services integrate their capabilities with an appropriate C2 information model and associated generic services.

3) These existing capabilities provide a natural test-bed for prototyped GIG services. For example, as the GIG delivers first generation authentication and authorization

services, these capabilities could be readily integrated within the existing information-centric architecture. This would give us immediate feedback into issues with how to interact with existing applications and users. Similarly, as GIG services become available, the similar services in our information-centric architecture could be replaced with the GIG approach. This again provides a natural test-bed as well as the ability to quickly utilize these services without requiring changes to the clients using the services.

4) Finally, the area of mediation between information/ontologies in different communities of interest (domains) is of great interest to us and promises to be an area requiring significant research and experimentation. Without this capability, the GIG will continue to provide a series of stove-piped systems. Our three existing information-centric systems (i.e., tactical (IMMACCS), JTF (C2TD), and seabasing logistics (SEAWAY)) represent an unprecedented opportunity to better understand the mechanisms that can be used to support integration at the information level. The ability to clearly flow information between logistics planning, tactical command and control, and the operation coordination systems would provide not only an extremely useful operational capability, but would significantly further our understanding of how to mediate between diverse yet cooperating communities.

6. Conclusions

The combination of information models and a generic services framework can be used to create a rich variety of systems able to represent and exchange information in terms that can be readily understood by both humans and machines alike. These approaches are essential to providing an open information-centric environment capable of handling real world situations - one in which agents can increasingly be delegated the responsibility for analyzing the increasing amount of data made available by the Global Information Grid.

Our work over the past six years has clearly shown that information-centric systems can be created and fielded using tools and techniques that are well within the skill set of today's developers. Further, we have shown that these information-centric systems can provide significant new capabilities while enhancing the capabilities of existing systems by providing them with richer information feeds.

Secure Origins: National Strength Through Security and Competitiveness

Hector Holguin
E-plaza, Holguin Group, El Paso, Texas

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

SecureOrigins

a Global Center for Secure and Competitive Trade

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

SecureOrigins

a Global Center for Secure and Competitive Trade

2,610 Plants Across 6 Border States

Maquilas comprise 78% of total export trade to Mexico

96% of Maquila Suppliers are U.S.-based

- Industry-Government Partnership
- Industry gains rapid supply chains
- Government gains secure supply chains

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

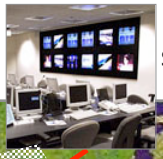
Secure Trade from Origin to Destination

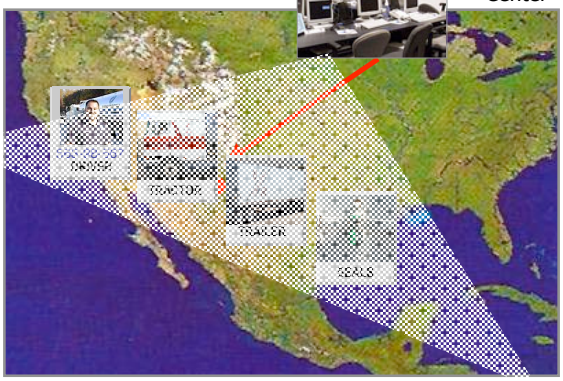
Web Cams

PDA Reader /Writer with GPS

RF Tag

Satellite Tracking

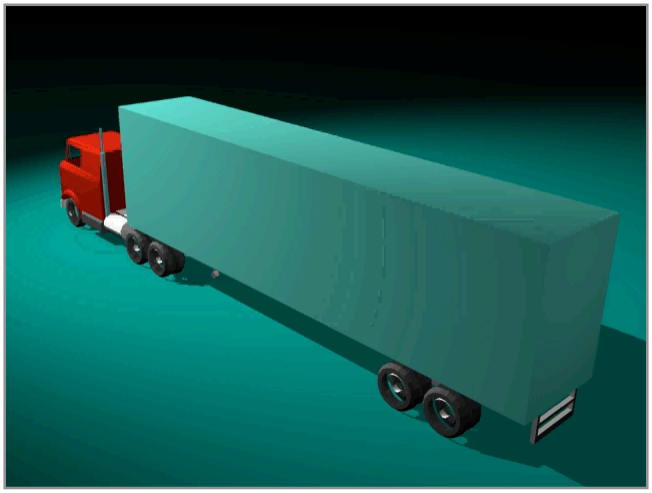

Global SecureOrigins Center



plaza™

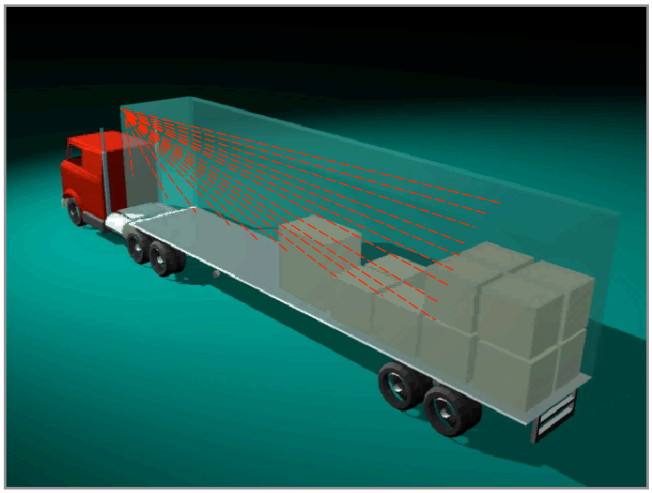
©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Secure Trade from Origin to Destination



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Secure Trade from Origin to Destination



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

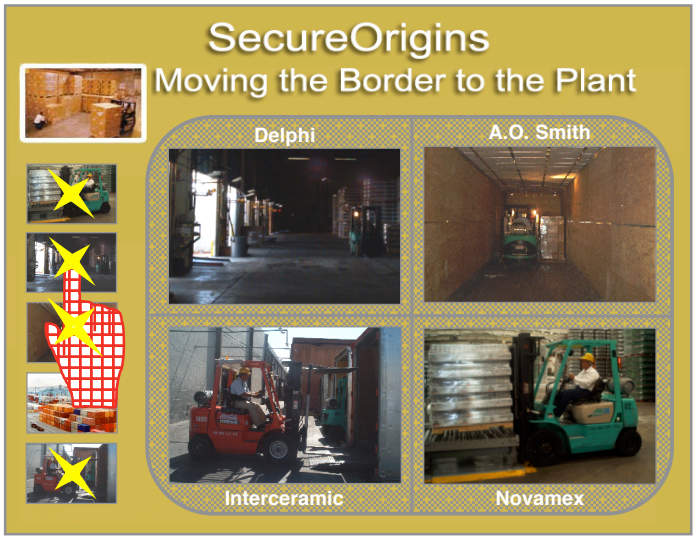
*e*Plaza

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Select a Border

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Access Plants



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

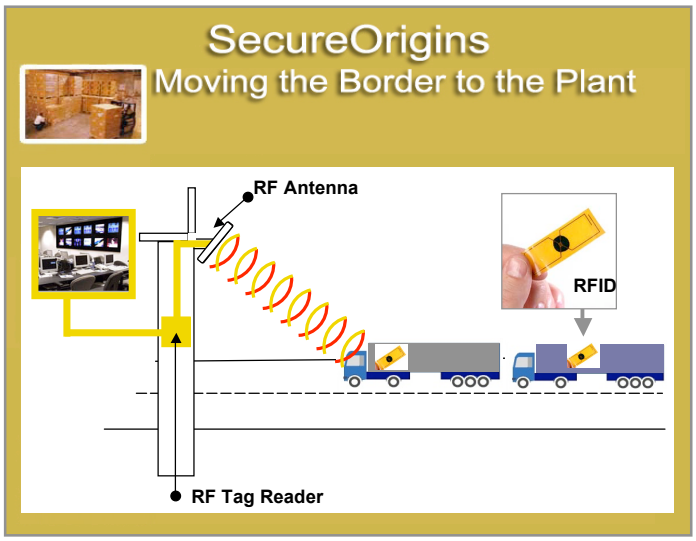
Loading and Sealing of Cargo

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Efficient & Secure Logistics

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Intelligent Logistics



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Satellite Tracking to Border Crossing

SecureOrigins

Moving the Border to the Plant

Geographic Positioning System (GPS)

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Centralized Communication

SecureOrigins

Securing the Supply Chain

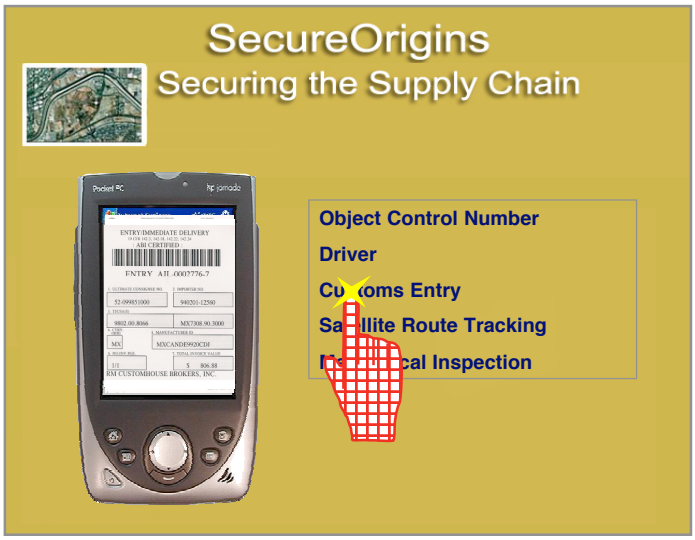
plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Mobile Field Inspections

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Document Verification



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Mechanical Inspections

SecureOrigins

TRUCK MECHANICAL INSPECTION

·Power steering	☑	O.K.
·Belts, hoses, lines	☑	
·Air pressure	☑	
·Wheels and rims	☑	
·Brake shoes and drums	☑	
·Lights	☑	
·Wipers, windshield	☑	*Chipped windshield*
·Extinguisher	☑	
·Engine, transmission,	☑	
·Rear differential	☑	

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Origin to Destination Visibility

SecureOrigins

Securing the Supply Chain

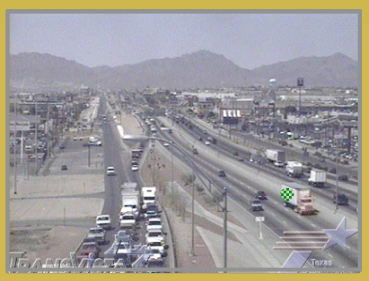
- Computerized Agents & Satellite Tracking
- Port of Entry
- Interstate Highways
- Maps and GIS
- Database Management

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Origin to Destination Visibility

SecureOrigins
Securing the Supply Chain



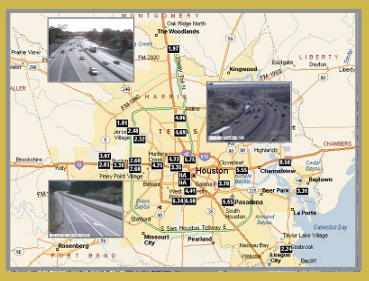
- Computerized Agents & Satellite Tracking
- Port of Entry
- Interstate Highways
- Maps and GIS
- Database Management

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Origin to Destination Visibility

SecureOrigins
Securing the Supply Chain

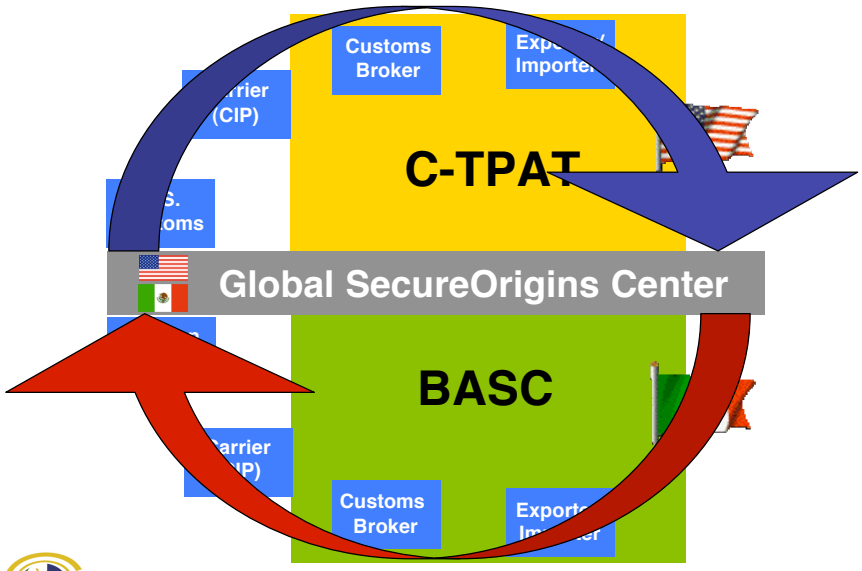


- Computerized Agents & Satellite Tracking
- Port of Entry
- Interstate Highways
- Maps and GIS
- Database Management

plaza™

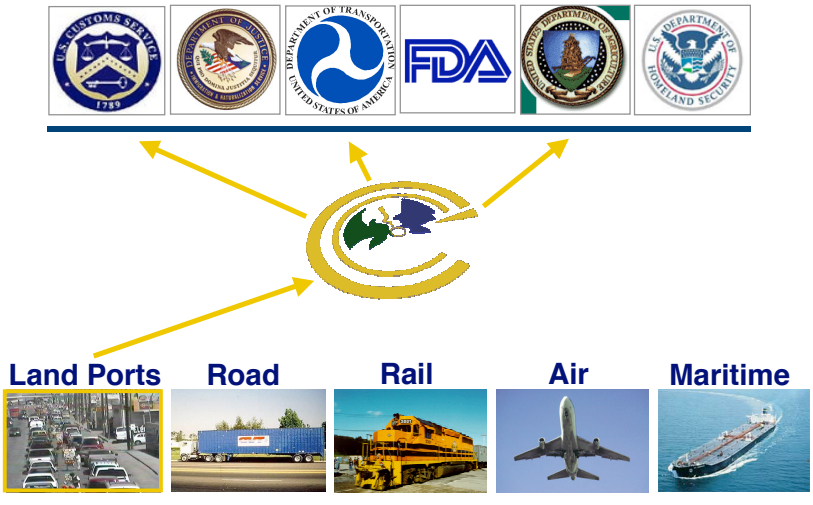
©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Securing the Supply Chain



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Intelligence Sharing & Multi-Agency Collaboration

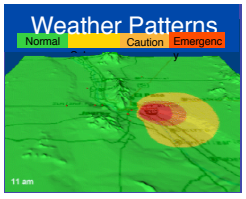


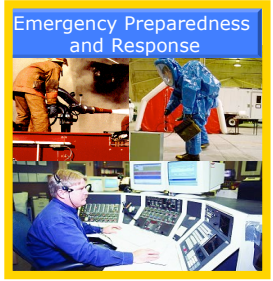
©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Information-Centric Technology in Action

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Homeland Security Notification and Response





©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Competitive Trade

Web Cams

PDA Reader /Writer with GPS

RF Tag

Satellite Tracking

Global SecureOrigins Center

- "Factory of the World"
- #1 User of the Internet
- Building the World's Largest Wireless Network

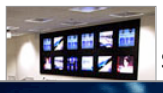
plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

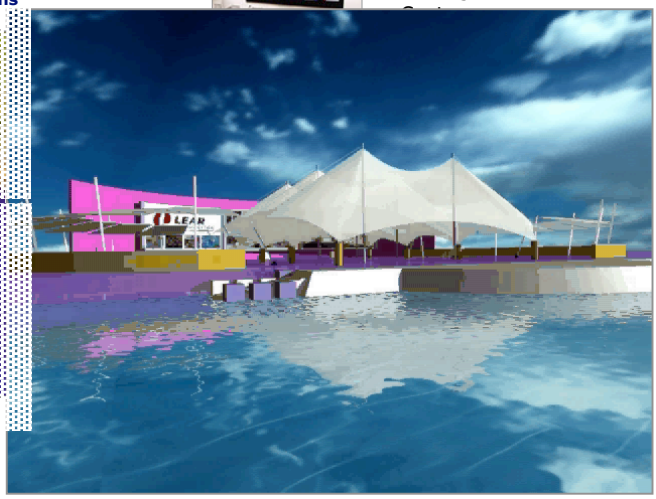
Competitive Trade

Value Added Services

- Advanced IT Communications and Collaborative Networks
- Intelligent Logistics
- Just-In-Time Supply Chain
- Web Cam Monitoring
- GPS Tracking
- Outsourcing/Help Desk
- Enterprise Solutions
- Business Center



Global SecureOrigins



High-Tech Jobs

- IT Consulting
- Network & System Administrators
- Technical Writers
- Software Developers
- Support Specialists

plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

SecureOrigins

a Global Center for Secure and Competitive Trade

Secure Trade –
Origin to Destination

Rapid Response System to
Security Threats

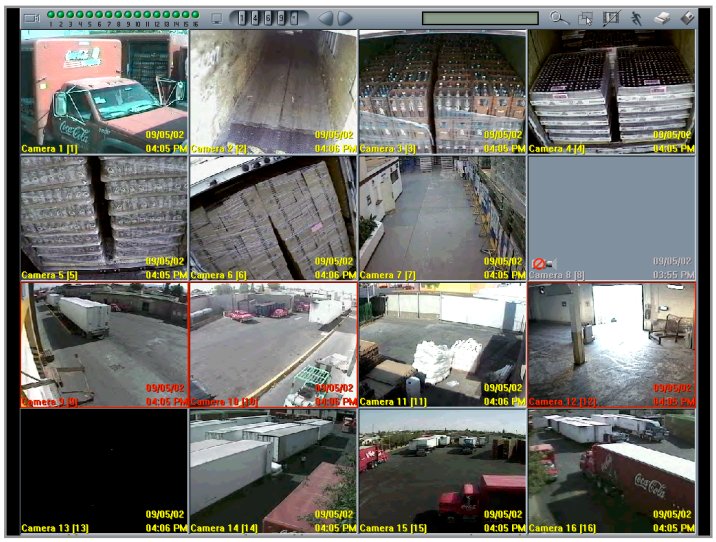
Competitive Trade

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

*e*Plaza

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Web Cams



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

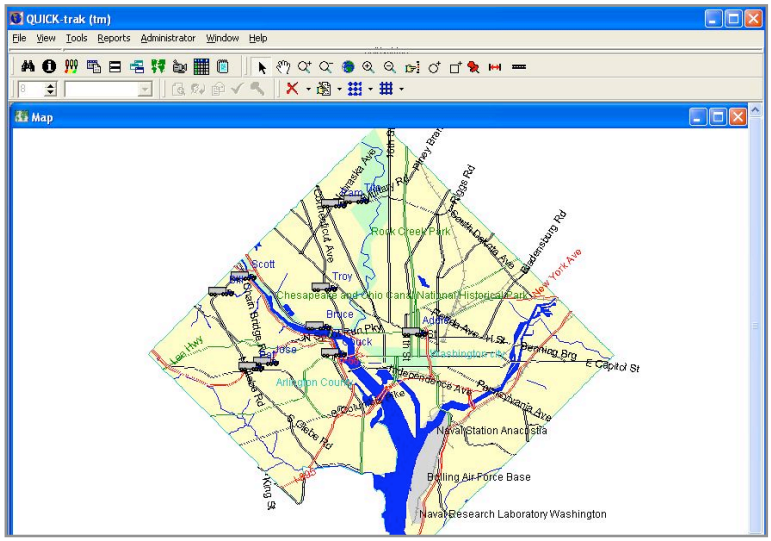
Web Cams

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

Web Cams

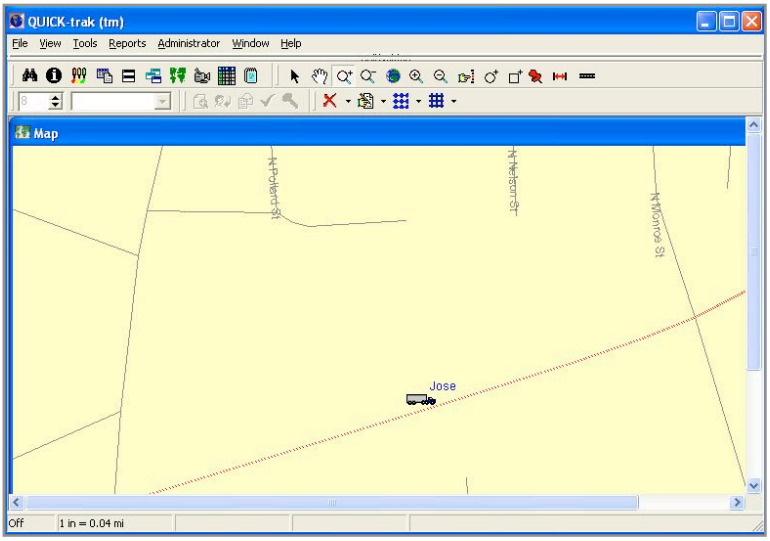
©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

GPS Tracking



©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

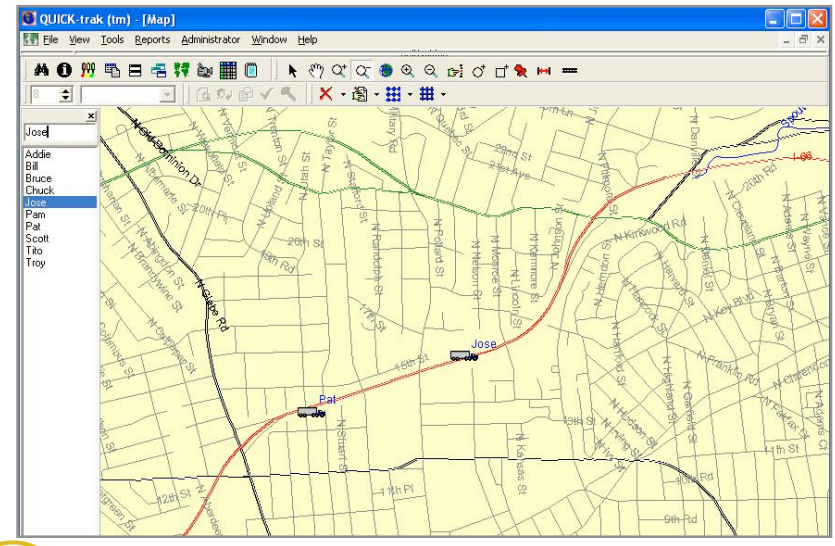
GPS Tracking



plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

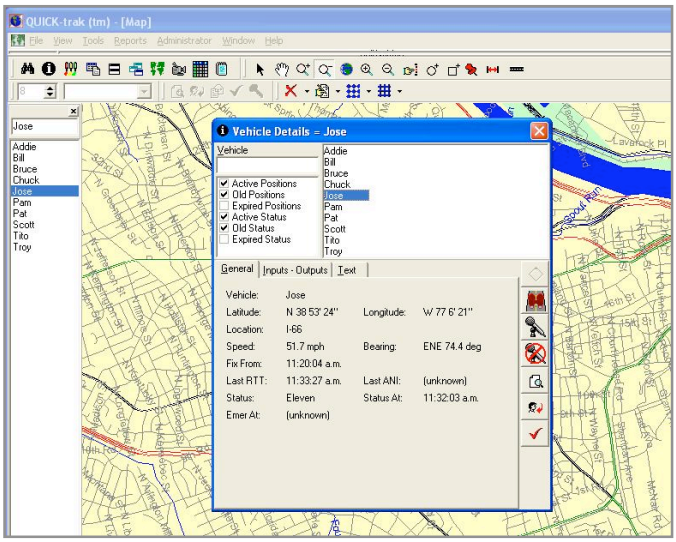
GPS Tracking



plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

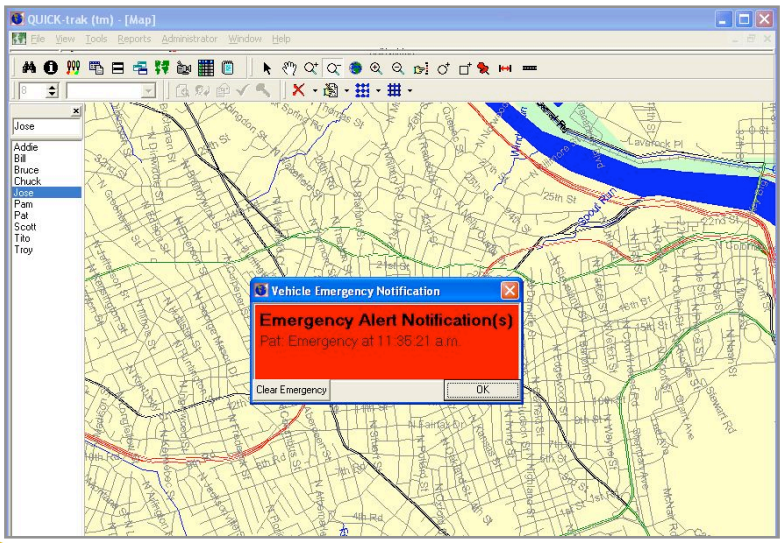
GPS Tracking



plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

GPS Tracking



plaza™

©2000 - 2003 Copyright HolguinGroup. All Rights Reserved.

A Data Strategy for the 'Virtual Border': Repurposing Commercial Information for Homeland Security Risk Assessment

Robert Quartel, Chairman and CEO, and **Eric Chasin**, CTO
FreightDesk Technologies, Dunn Loring, Virginia

Quartel: Before we get started, let me give you a little background on FreightDesk Technologies. The company was launched about four years ago, backed with venture capital, with the goal of providing a collaborative platform for freight forwarders. Why? Because eighty five percent of all international trades are managed by an intermediary. The goal was to technology-enable the middleman rather than disintermediate him, which was the strategy of many of the failed dot-coms of the period. Two years ago we split the company along technology lines – the original was a Microsoft-SQL server model; and today we have an advanced Oracle Java J2EE technology data architecture model and software that fundamentally captures all of the data related to an international trade in any form, from any mode, and instantiates it against a single shipment. Eric Chasin, our CTO, who designs the software and is involved in managing a number of our projects is here with me and will talk about some of our experiences a little later.

We will talk about a couple of things today; supply chain security versus shipment security, a little about both the data and the data model, and about application of the model to real world experiences. Currently, we are probably involved in more projects like this than anybody else, working with TSA, FDA, DOD, ONI, Homeland Security, as well as a couple of tradelanes in Operation Safe Commerce program. Our role in each of these projects is to collect the data into this platform, organize it so that it can be re-purposed for things like profiling, as well as other uses. We will also discuss some of the challenges we face and talk about some of the lessons learned.

One of the biggest problems in any of these projects is in capturing the data related to the international trade transaction and in actually connecting it to a particular shipment for analysis.

I have already touched on this, but basically we have a platform of technology that is actually being applied, that is scaling well. Eric will probably talk a little bit about this, but right now we are running over a million documents through the system a night. There are roughly 50,000 shipments that arrive in the United States every single day which means that there are about a 250,000 shipments that move around the globe in any given day. This translates to about 2.5 million to 3 million shipments in motion at any given time when you consider that international shipments take anywhere from 7 to 20 or more days to reach a final destination. Therefore, about a third of things moving on ships globally are going through the system, and as much data as that is, it is probably less in a year than a major bank processes in a night. While people can tell you this is highly complex and requires mammoth systems, the fact of the matter is that the scale of the issue is not the problem.

I began by saying that about two years ago we had split the company along technology lines, partly to go after other market segments. Just weeks afterward, September 11th hit and ten days

later I woke up at 3:00 in the morning thinking about ocean containers and realized, "Whoa, you could put a Stinger in a box." From this idea we developed a concept which I called "pushing the border out," that is, the notion that you could create a "virtual border" by capturing the data related to the trade transaction much earlier than it was currently being captured and analyzed. We took this concept over to our friends at LMI, with one of the partners of which I had done some work in the past, and we and a number of others developed – after some quick study – and sold to some of the key players on the government side this notion of a virtual border.

The animating concern was that if you are bringing a cargo into the US, it's already too late if it contains a bomb – because either the port is a potential target, or because the port is a portal to another part of the country. As a note to bear in mind, while the focus initially was on containers and we tend to talk about the issue in these terms, the problem really encompasses more than containers: It's really about anything that moves, by whatever means, by whatever platform or conveyance, in or outside a box. Today, the whole concept of pushing the border out is one of the five pillars of homeland security strategy.

At the heart of all of this is that you have to start with a big haystack, making the assumption that every shipment has the potential to do damage – but it's really an unacceptable demand on the system to physically examine every cargo. So how do you determine if you should stop a cargo overseas? If you inspected everything in a single ship of 4,000 containers, a ship that today offloads in 18 hours could take 30 days. The job is to find a way to monitor the cargo without unduly sacrificing efficiency. Our notion here is that by creating an electronic data border it allows you to assess risk and focus on cargo which you actually want to inspect, before it makes the final leg to the US. While there have been a number of technologies thrown at the problem, there is no silver bullet: The solution is part technology, part people, part process, part data, and the integration of these and other systems.

One of the key insights in this whole process and the way we do it today is that customs is that while US Customs, which is in charge of the problem at the moment, is used to capturing shipments at the border for compliance purposes – the valuable information is contextual, rather than content-oriented information. Nevertheless, Customs is used to dealing with this as a compliance problem, at a single-point, and as a border issue.

They certainly have accepted the notion of the port as a catcher's mitt…eg, an appropriate place to stop a cargo. But, again, it's treated as a compliance problem that focuses on whatever it is or is said to be in the container. So, they continue to think that you physically inspect it in Rotterdam, and, once you've done that and let it go, that's the real end of the process. But, the reality is there is no such thing as a shipment here or a shipment here, with a concrete stopping point. Shipments are really part of a fluctuating supply chain, in constant motion, moving through a process that operates in an environment with a lot of other exogenous things being thrown at it. And, of course, a shipment has to start somewhere, and that is really the notion of supply chain data and its manipulation and analysis. Now a question for you -Where does it start? It doesn't start at the factory overseas. It starts here, in the United States, when somebody orders it.

One of the other challenges in collecting the data related to an international trade is that it comes at you from all different directions at different times. While we all tend to think of it as a linear process, it's really non-linear. But for analytical purposes, you have to formulate it into a characterizing sequence, which is the exact purpose of our data model.

Here's one way to think about this: A freight forwarder in Boston calls American President Lines in February and tells them he wants to move 20 containers in September from Rotterdam to New York. The ocean carrier now has in his system has a pre-booking but doesn't know what's in the container or who it's for. All he knows is that it's for the freight forwarder. The freight forwarder doesn't know who it's for except that he knows historically, he's done it in the past. So now already you have two separate streams of data, both with large unknowns, but with a high level of situational predictability. Now, in May in a different part of the world, the ERP system for a company's manufacturer in Thailand says historically they've had orders in August for September, so they need to start ordering raw materials now. Well guess what -- this order produces data and thus the process has started. And, while this company has decided in May to order materials or sub-products from another company in Asia, they don't know for certain whom the order is going to come from so that's another data stream. What you're looking for, when it finally starts to move, is how to put all of that disparate data together in a meaningful way. All of that data's already there, but it resides in the systems of the people who created it and only a small fraction of that gets reported to the government or anyplace else.

Someone earlier was talking about the notion of the idea of the acronym, GIG or one of those processes where basically everybody's going to throw their data out into a system for everybody else to use and collaborate. The problem in the commercial world is that nobody wants anybody to have any data on their transaction except what they need to know about the handoff. There are competitive reasons for this obviously so the task is as this data comes at you, to start putting it in order, against what you know from some other parts of the supply chain. You may have moved from here to here but the data from that move doesn't arrive. That data might actually arrive before an event that happened back here. So what the data model does is capture the data, starts to put it in the order of the advance, link it to all the parties that were involved, and then you can start re-sequencing and moving forward with profiling and analysis.

Cargoes begin as a shipment, and shipments begin with orders and bookings. This is not a linear process, however, and it can be extremely random even though people tend to think of it as being linear. You buy something, it gets ordered, you do this, it does that. It doesn't work that way when dealing with high transaction volumes. Once you get the data you're going to run it through algorithms looking for anomalies. You've heard some talk about data, the data capture itself, how you do it, where you do it, and from whom you do it, and this is a critical part of the way you can analyze a trade transaction.

This is a map of what a typical international trade flow looks like that we and others produced for TSA. The typical trade has 20 to 25 different parties involved, beginning with buyer, seller, ships, trucks on both sides, insurers, banks, customs on both sides of the water or land border, along with 30-40 documents, and 200+ data elements. What this does is generate yet another table of data which I will discuss briefly. There are hundreds of data elements that drop out of this process, some over and over and over. I will show you this slide in a few minutes about how

much is electronic, and how much is not. We also tend to think of everybody as being electronic, which is not the case, so again the data model also needs to be able to take information that's not electronic. It might be keyed, and we got into this as a commercial company, but in point of fact, this is hugely applicable to the government problem because in fact in order to solve the problem you have to understand and replicate what's going on the commercial side.

A shipment is defined by all sorts of data elements coming from all sorts of sources being thrown at you. The involved parties create purchase orders, bills of lading, and proofs of entry. But how do you find out the contents or who touched it? Some information may be in packing lists, some of it on bills of lading. So how do you find out the routing, which is the transportation part? You obtain that from the carriers and from a several other documents. You have load and discharge documents at the ports. You have comparable kinds of things, rail and so on and so forth.

One of the problems with the way Customs is thinking about this right now is they at least publicly believe if they can get everyone certified under a supply chain program…C-TPAT in particular…and that if a process is locked down and repetitive, happening over and over and over again, everything will be copasetic because you know how it will behave. In reality, every shipment is unique, like a snowflake. It's a kind of a sequence of events in time, some person is going to be different, some sailor on the ship is going to be different, some truck driver is different. They travel a little slower, but if you're thinking about this as an analysis problem, every one is different, again, like a snowflake, existing only in a limited time framework.
This is the notion of the virtual border. Prior to about a year and a half ago you had the warehouse, the ship sailed and boom here's the border in the United States or overseas in the other direction. The goal of the virtual border is to push all the data capture which is on the other side over here. Prior to the 24-hour Rule, many documents and most of the limited data available to the government from manifests were reported to Customs well after arrival of a cargo. The notion of the virtual border is to capture as much of the commercial ability as you can, which is much more robust than what's in a government system, and integrate this well before a cargo gets into final motion to produce pre-emptive results.

One of the proposals that we made two years ago was to require that the data be reported 24 hours before you load the ship overseas. The number 24 was plucked out of the air and in reality you ought to be able to do it in 24 minutes, not 24 hours. However, the government and customs systems require that you report your information today in the electronic manifest. Eric will talk a little bit about why this is a problem. A manifest details the shipper, the consignee, the routing, very high level cargo description. Customs now also requires integration of the bill of lading data into the manifest, which in and of itself causes a problem that they don't seem to understand: The latter are commercial documents and the former, the manifest, is a transportation document. All an ocean carrier needs to know or a truck carrier or a rail carrier or anybody else is, where they pick it up from, who they give it to, what date they pick it up, what date they deliver it, and under certain conditions they need to know weight. It used to be required that they know weight, but they don't really need to know weight on a ship of 4000 teu's any longer. They also need to know if it's hazardous material. One of the unfortunate artifacts of the constraints the government is under, which Eric will discuss, is that they're trying to shove a lot of stuff through the manifest that doesn't belong partly because they don't understand the

process and partly because they're constrained by legacy systems, and partly because they're still fixated on compliance regimes.
Now, at this point, I'm going to pass it off to Eric.

Chasin: First a couple of quick questions. How many people are familiar with the documents involved with international trade? How many people are familiar with the electronic technology that is state of the art in transportation called EDI? If I had asked the percentage of information moving which is on this well-accepted standard EDI, what would you guess the volume of electronic data that moves today is, 50%? %90? With companies like Wal-Mart and Kmart, what would you think the amount of electronic information flowing in the transportation world would be? Normally less than 3%. Looking at the current state of the transportation world, US Customs requires everybody to follow a manifest. This manifest was never really designed for intelligence purposes or information gathering, but was really defined for a carrier to submit basic information about the transaction; when they arrive at a port, what's on that vessel, how many containers they are offloading, are these containers going off to LA or are they going all the way into Canada or Mexico by rail. So the challenge that we address came out of the commercial world, and it came out of a small company called Phillips Electronics. They wanted to know actually what was inside the container when it arrived at the port, because if they were having a sale for wide screen TVs at Best Buy and you had 20 containers coming in and only one container had wide screen TVs, that's the one that you'd break bulk and air express out. So the whole goal of the process is to discover what's in that container.

The next thing we had to do is address who else was part of that transaction. We took a commercial product that was there to identify who and what was in a particular shipment and expanded it out, so the current state of the art is a document called an AMS manifest. This is filed 24 hours before departure. If I gave you one document and you had to profile off of this document, how well do you think any profiling engine would work? It only had one version of the truth to look at as opposed to the 26 documents that were floating around somewhere in the life cycle of that shipment. Had other information that either contradicts, supports, adds to, or embellishes that one transaction been available, you could collaborate the information given by a number of sources. Of the 50,000 shipments that come into the US that are containerized, our technology has the ability to take massive amounts of messages from disparate parties, port operators, exporting countries, ocean carriers, rail carriers, corporations that do purchase orders, and advance ship notices. We can then take all that information, capture it in a rapid and efficient manner, aggregate it up and build a record that says you now can profile off of something that represents 20 or 30 other messages and monitor where the values contradict.

Is the container the threat? I've never seen a steel container blow up by itself. I've heard of spontaneous combustion, but I've never seen a container go "boom" in the night. What you're really concerned about is what's in it, who touched it, and basically where it's been, because strange things can happen even if you secure the port of Singapore. The minute it goes outside of the port for 24 hours there are a lot of people that can touch it, so what we tried to do in our system is deal with the shipment, the order that it supports, and the involved parties who touch it. That includes the bank, the ports, the crew, the vessel that it's been on, the route it was supposed to take, the other feeder vessels or trucks that brought it there, the currency that it could possibly be paid on, and every event that has happened throughout the life cycle either of the shipment,

the vessel or the container or package. Now if I take a look at US Customs, they process 50,000 messages a day. We process on those 50,000 and 2 or 3 million messages a night relative to containers that move. So the data volume that you have to aggregate is just a massive amount. Now we add in other technologies, transponders, and video cameras but the problem you run into is, you're drinking from the fire hydrant now. So part of the concept is you have to aggregate, you have to analyze, you have to basically have some pre-alerts because no analyst, no intelligent analyst, no border guard, can digest that much information as it speeds through the system…next slide…

Quartel: I'm going to take one minute on… that is an anomaly…

Chasin: The anomaly here is you know people are concerned about the origin of the shipment. The container moves out of the UK it actually has been declared as cigarettes. It goes to another port, probably in the port of Panama, and nothing changes in the container; however it leaves the port, comes back into the port where it's now manifested as a set of textiles. So quite often it's not the actual threat of that one shipment, it's what happens from that transshipment point. The other issue Rob mentioned is that if I'm very sophisticated I can bring three inert products or non-hazardous products, bring them all together at a certain point, put a small explosive device in and then have a very big economic disaster.

Quartel: And by the way, this is a key point as well, we tend to think that if we know what's in the box and it's legal, and all of the parties to that transaction were themselves legal, and we secured it along the way physically, everything's copasetic. The reality is, imagine someone breaking into a ship booking system, an ocean carrier booking system or rail booking system and slamming two or three hazardous materials together that normally would be at different ends of the ship or another item intersecting that process. Again, it's not just the shipment or even the life cycle of that shipment per se, but instead all the other intersecting events.

Chasin: Next slide…So what we do is we have a software technology that processes all the disparate messages that exist in the system, and they can be EDI, they can be Flat files or xml files. We also provide an application that facilitates the process. If I said 3% is electronic, that means 97% of the data exists probably in phone or fax, so if we're going to implement a stronger virtual border, you then actually have to facilitate all these international parties with an application where they can contribute data into the system. A perfect example is across the Mexican-US border. If US Customs mandates that you need to file this new data electronically and I'm a small supplier, not the big supplier, I have to basically pre-file if I can have the US government facilitate that process, you don't get compliance from the system. If anybody who's in noncompliance is instantly a high threat, incidentally they're a high threat, and the cost of securing the port goes exponentially high. But there's technology out there and certainly with the internet that it brings the cost down where it is enforced with regulation and compliance and technology you actually can secure the border by an information base, because again, you don't want to drink from the fire hydrant. You want to get to the point where you can do some network analysis and some profiling before it gets to the border.

Quartel: Let me make another quick additional point to that from an economic standpoint. Transportation trade is 80-20… 80% of companies do 20% of the business, 20% do 80% plus or minus. That means really 80% of the transactions are by small players even though 80% of the value is big players. So if you can't solve the small player's problem of the 97%, then you have an even bigger problem.

Chasin: Next slide…So what we do is… we take all these different messages, and currently right now we probably process about 23 different types of messages. We build them into this one extremely sophisticated data set, and then we provide this data set to our partners on these projects that actually run algorithms against it. You can do link analysis, you can do network analysis, you know what other shipments do these people ship to, what countries are they tied to, what bank are they tied to, and the power that we have is we build those relationships in the database to get the performance up and entirely scalable, instead of trying to do it with kind of a query tool which would mean massive computing power. Next slide…

These are the projects that we're with… I'll give you a little bit of experience. We have one project that had one source of data, and that source was the carrier, so we saw the shipment in their view of the world, and their view of the world is "I don't really care what's in it, all I want to know is what I'm going to charge for this container… it's going from point A to point B, and after it goes to point B, I don't really give two hoots where it's going after that… as long as people pay for it"… Then we had another project that was global in nature that said, we're going to have all these countries in the world and all these ports in the world report their data, whatever data that they naturally generate. That project was very powerful in the sense that we could actually track where a container's been, how long it's been there, did it get lost out of sight for a while, are there two different involved parties to find on this shipment, and are these people on a watch list. So what we found out is from two different projects, one where one organization provides the data, versus that about 56 sources providing the data, the more data you've got, the more reliable your profiling capability and better intelligence that you had off of that… next one…

Alright, the reality is there's a ton of data. The reality is no one calls the port of Hong Kong the same thing. If I actually want to know what's moving from Hong Kong to LA I have to have the capability to resolve and normalize all this information throughout the world and tie it back to a single record. So we've created some technology that does that because you really don't want to have a scatter chart. Give me a minute, I think we're almost finished… so the reality is data exists but it's not easily accessible… next slide…

Regulations and policy definitely impact and improve our ability to collect data and with the US Trade Act and the MS 24 hour where we have more compliance… I want to go to the next slide…

Quartel: Give me one second… I'm going to take one second to mention the second bullet. One of the biggest problems is being able to manage data in a way that operates effectively. Here is the way the commercial system operates. Customs has a system and they're constrained by that and everything they do has to be crammed through that single system and manifest system… chart…

Chasin: You take a look at this chart that came out of one of our projects. There are massive amounts of data out there, all the way from a purchase order, to cargo descriptions, to event messages, and it's all controlled by about 40 different involved parties, but truly there is very little that's electronic today. So one of the things that policy has to address is how do I go out and allow people to participate in a supply chain and tie their pieces of information to a common record, which doesn't exist today. Purchase orders and advanced shipment notices and bills of lading exist as a single snapshot of data that in the industry and in the business process are not related. You have to be able to relate all that information to a common type record and we do that in our aggregation engine. I think from a government policy standpoint, there's going to be this control number that's going to be set up at one point to track both inbound and outbound shipments to the US… next one… we need to finish this up…

Rob: This is what I started to talk about earlier. There are two major rules out there in how to make this happen. We've talked before about software and controlling the logistics processes, and having efficiency gains as part of the benefit to industry, as well as security gains to the public. The reality is most businesses don't think that they're affected by terrorism, and most don't have enough money to buy something where the solution is two or three years in the future. It's a typical software problem. When you look at this problem from a government or public policy standpoint, in order to get greater supply chain security and visibility, in the end the government will have to mandate it. Almost none, or only a few companies, would do it voluntarily.
Everybody in the Customs side of the equation is looking for a solution way out into the future. They're building this big enterprise system called ACE and hoping that when completed it will solve their problem. However, the reality is that the problem exists today. We should be forgoing the enterprise solution and looking to experiment, build incremental solutions that can help us get a handle on the problem TODAY.

One of the most important lessons we have learned is that we don't take enough advantage of the commercial data environment. This is a process that just spews data, but Customs in particular utilizes only a small amount of what's out there. They continue to analyze the limited data they have with limited analytics…using a simplistic rules-based system that, frankly, has failed us in the drug arena - rather than a learning-based or analytical system to figure out whether cargo may be dangerous. The second lesson is that we need to find ways to make data capture from all participants more efficient. We can try to get the industry to do these things voluntarily, but as I said earlier, a lot of this will need to be mandated. We have also talked about the need for an ID to link all collected data to a shipment and then to process the information gathered. Finally, the government needs to bridge the gap between theory and practice, which is what I think we are beginning to do for DOD.

Any questions?

A Regional Supply Chain Simulation Model Using Artificial Intelligence

Dr. Larry Mallon, Director, CITT
Long Beach State University, CA

Presented at the 5th Annual ONR Workshop
Quantico, VA
September, 2003

OUTLINE

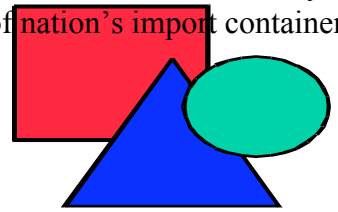
- Objective: Present collaborative information-centric approach to Southern California regional supply chain management, commercial and military goods movement, and rapid deployment
- Center for International Trade and Transportation
- I - Regional Supply Chain Simulation model
- II – On dock rail movement simulation and distributed logistics
- III - Rapid deployment simulation and agent based collaborative supply chain management
- Next steps

Center for International Trade and Transportation

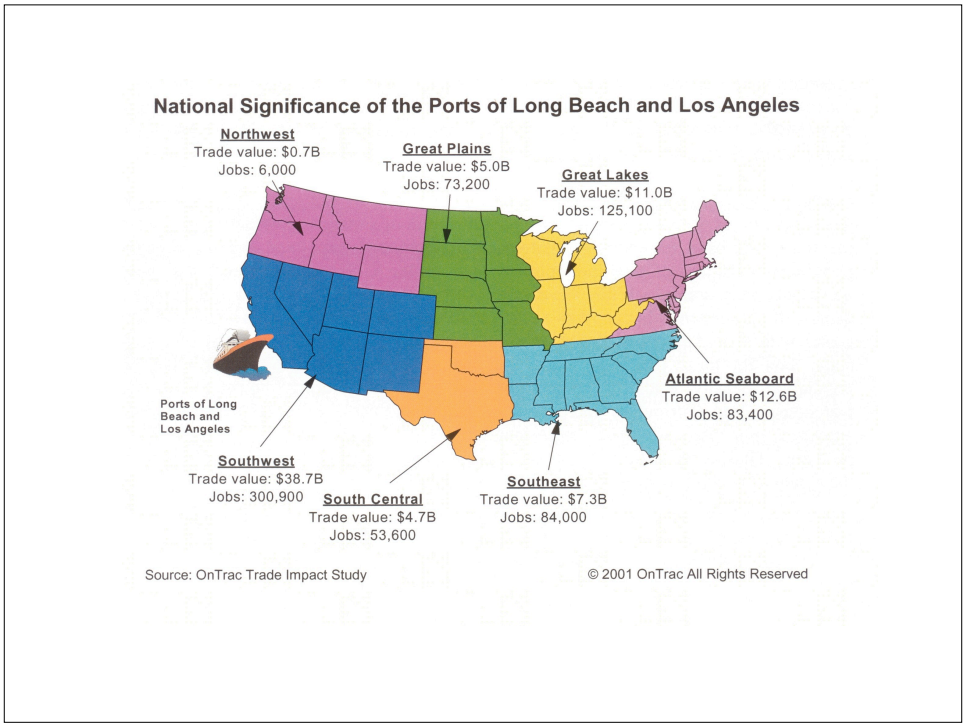
- Established in 1977 at California State University, Long Beach, California
- Designated a university transportation research center by U.S. Congress in 1997 (TEA 21)
- Supported by USTRANSCOM and Now ONR under High Speed Ship Design and Agile Port Demonstration, Transformation and Force Protection
- Specializes in intermodal transportation studies and integrated logistics research, education, technology transfer, and homeland security

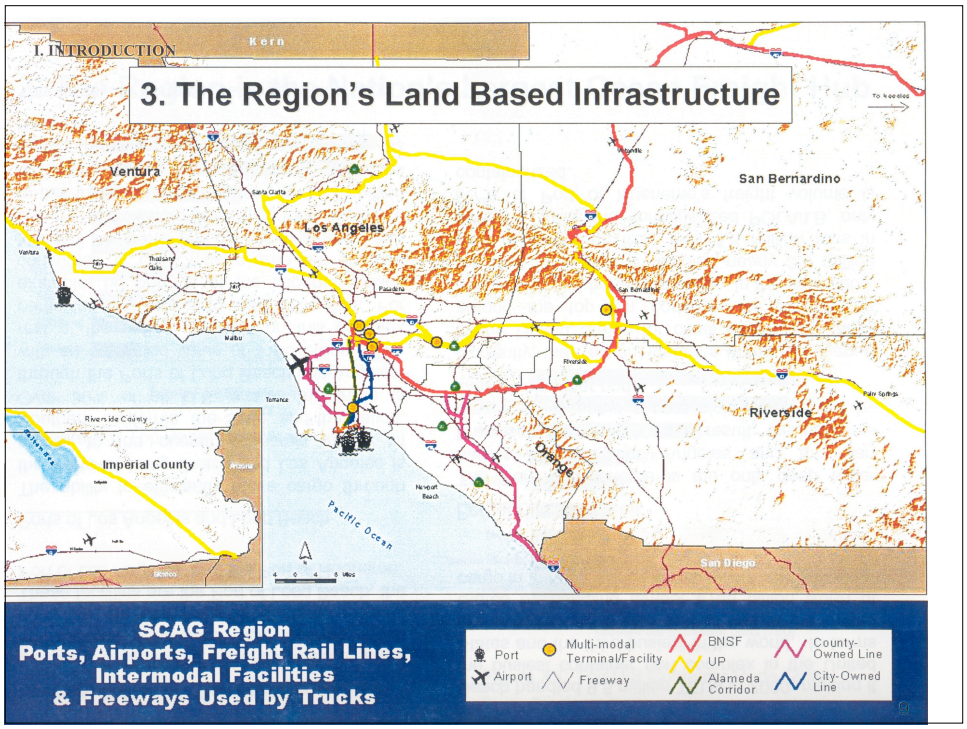
Commodity Freight Flows:

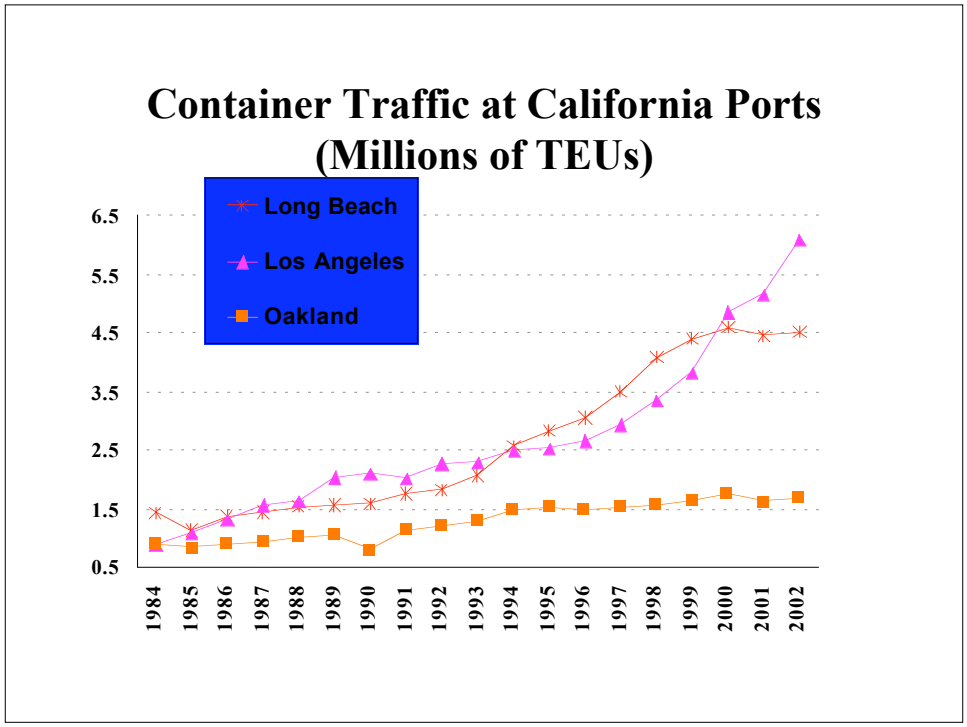
Southern California is Gateway to 35% of nation's import containers

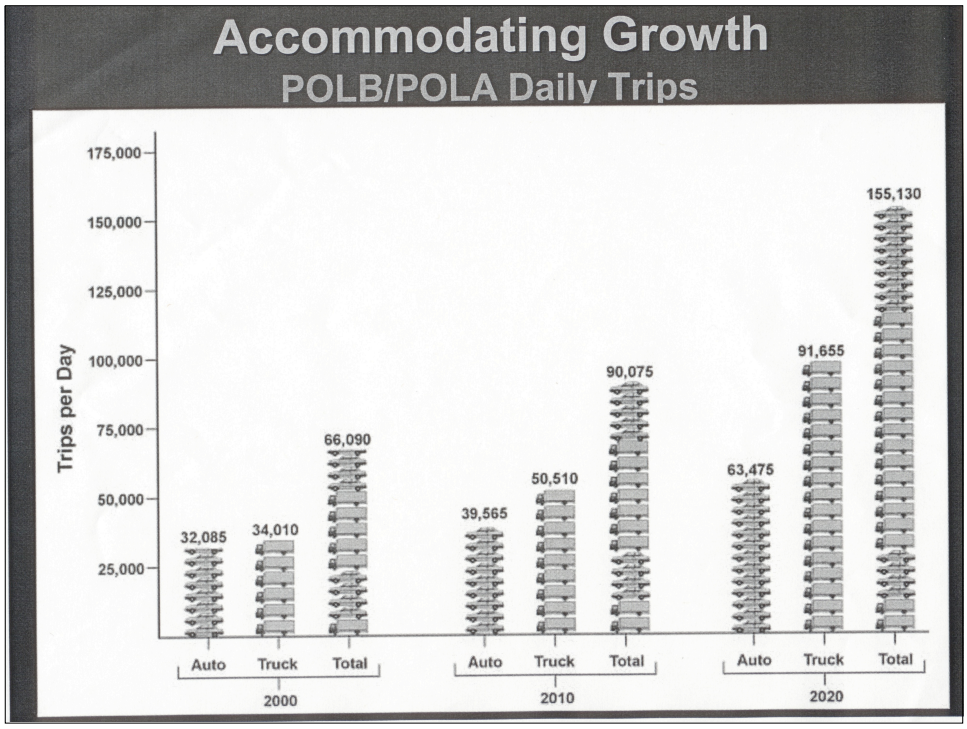


Ports of Long Beach/Los Angeles
110
710
Alameda Corridor


National Significance of the Ports of Long Beach and Los Angeles
Northwest
Trade value: $0.7B
Jobs: 6,000
Great Plains
Trade value: $5.0B
Jobs: 73,200
Great Lakes
Trade value: $11.0B
Jobs: 125,100
Atlantic Seaboard
Trade value: $12.6B
Jobs: 83,400
Ports of Long Beach and Los Angeles
Southwest
Trade value: $38.7B
Jobs: 300,900
South Central
Trade value: $4.7B
Jobs: 53,600
Southeast
Trade value: $7.3B
Jobs: 84,000
Source: OnTrac Trade Impact Study
© 2001 OnTrac All Rights Reserved


I. INTRODUCTION
3. The Region's Land Based Infrastructure
Kern
Ventura
Los Angeles
San Bernardino
Riverside
Orange
San Diego
Imperial County
Riverside County
Pacific Ocean
SCAG Region
Ports, Airports, Freight Rail Lines,
Intermodal Facilities
& Freeways Used by Trucks
Port
Airport
Multi-modal Terminal/Facility
Freeway
BNSF
UP
Alameda Corridor
County-Owned Line
City-Owned Line


Container Traffic at California Ports
(Millions of TEUs)
Long Beach
Los Angeles
Oakland
6.5
5.5
4.5
3.5
2.5
1.5
0.5
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002


Accommodating Growth
POLB/POLA Daily Trips
Trips per Day
175,000
150,000
125,000
100,000
75,000
50,000
25,000
32,085
34,010
66,090
39,565
50,510
90,075
63,475
91,655
155,130
Auto
Truck
Total
2000
2010
2020

Regional Supply Chain Simulation Model

- Macro-level, multi-modal simulation model
- Uses information flow in form of Electronic data interchange (EDI) data elements as surrogate for physical tracking to provide in transit visibility and to support collaborative regional supply chain management
- Multiple server, multiple queue
- Customer-driven transit times to benchmark hierarchical time-definite freight flows as methodology for optimizing regional goods movement

Model and Simulation

-A model is a logical description of how a system, process, or component behaves. Instead of interacting with the real system, one can create a model that corresponds to it in certain aspects.

-Static models describe a system by measuring system flow or capacity or units through relationships (database) or a single computation (spreadsheet) with performance measured by summing individual events, e.g. dwell time for a single container.

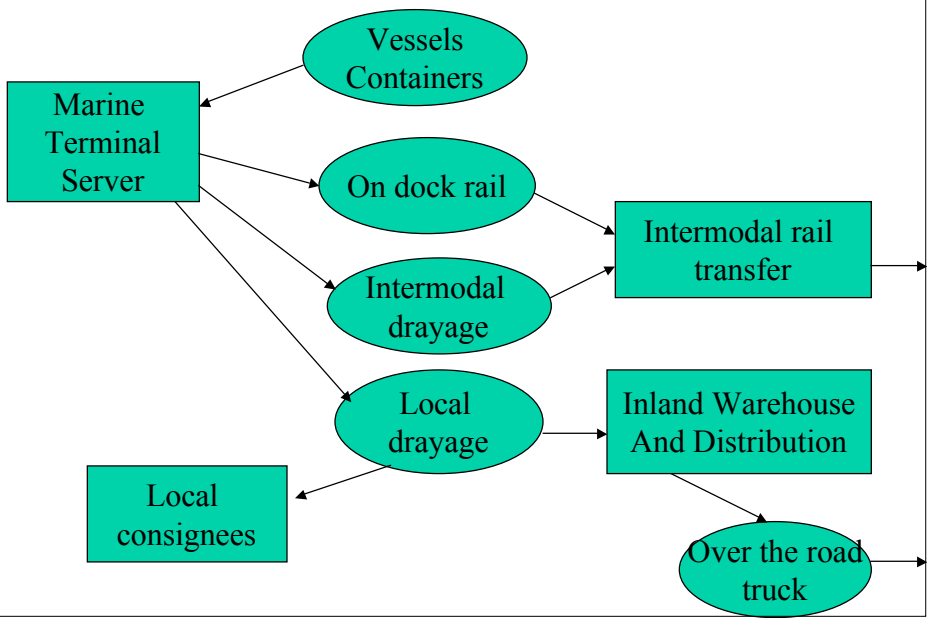
-Simulation or dynamic modeling is a time-based representation of a system and carrying out experiments on it. The purpose of these experiments is to validate the model by determining how the real system operates and to predict the effect of changes to the system over time. “What if ?” changes in marine terminal operating hours or infrastructure capacity (I-710).

Simulation is defined as the process of designing a mathematical or logical model of a real system and then conducting computer-based experiments with the model to describe, explain, and predict the behavior of the real system.
Scheduling or queuing problems deal with benchmarking processing times of work flow or separate queues comprising a system, given constraints on personnel, equipment, and facilities.
Simulation is a powerful tool for the analysis of scheduling problems, algorithms, and policies, simulation and scheduling or queuing analyses were the motivation for the simulation study

Regional Supply Chain Simulation Model

A multiple server and multiple queue freight transportation system susceptible to routing, scheduling, dispatching, equipment management, capacity utilization and surface transportation infrastructure optimization analysis.

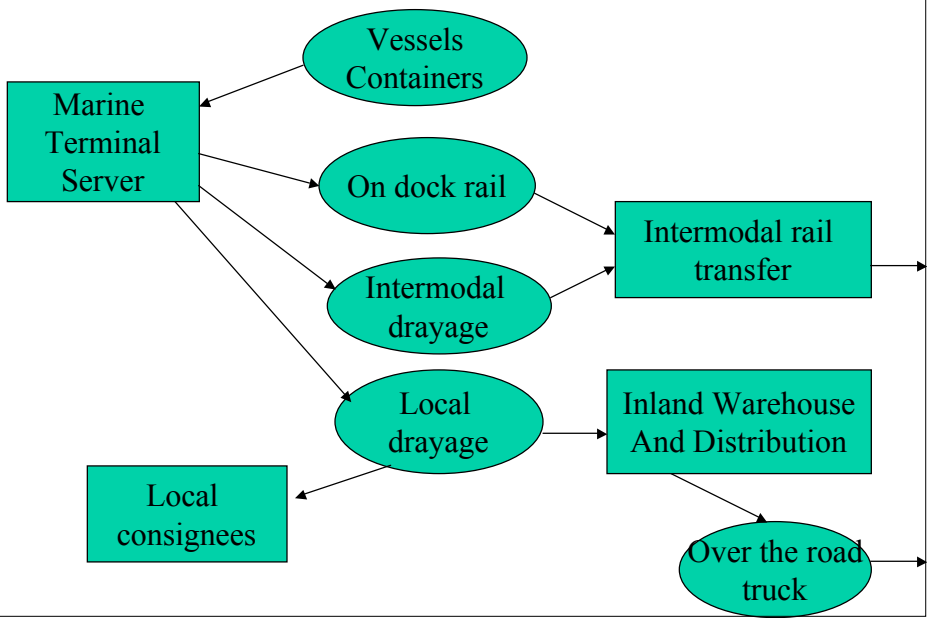
REGIONAL GOODS MOVEMENT SUPPLY CHAIN PLANNING MODEL



Throughput velocity

- According to the laws of physics, speed like productivity is a one dimensional metric measuring distance traveled over time
- Velocity on the other hand is the change in displacement over time. The difference is that a measure of velocity includes both speed and a direction as in a vector.
- Throughput velocity represents a combination of the spatial factor of displacement and direction measured in throughput per acre and the temporal speed factor of average dwell time for import, export and empty containers, trailers, or rail cars
- Applicable as a benchmark of efficiency in the use of system capacity in optimizing the flow of regional goods movement

REGIONAL GOODS MOVEMENT SUPPLY CHAIN PLANNING MODEL



Servers and Queues

Three Sets of Servers:

- 15 Marine terminals
- Intermodal rail transfer facilities (3 international: ICTF, Hobart, East LA; and 4 domestic: Commerce, Industry, LATC)
- TPL warehouse and distribution, and trans-loading (carrier, truck, independent)

Seven Wait Queues:

(1) Berth (vessel arrival and departure at marine terminal)
(2) On dock rail ramp
(3) Marine terminal gate (intermodal/local dray, pre-mounted minibridge, store door,empty returns)
(4) Intermodal rail transfer facility gate
(5) Intermodal rail staging/scheduling
(6) TPL transdock/transload

Regional Goods Movement Freight Flows

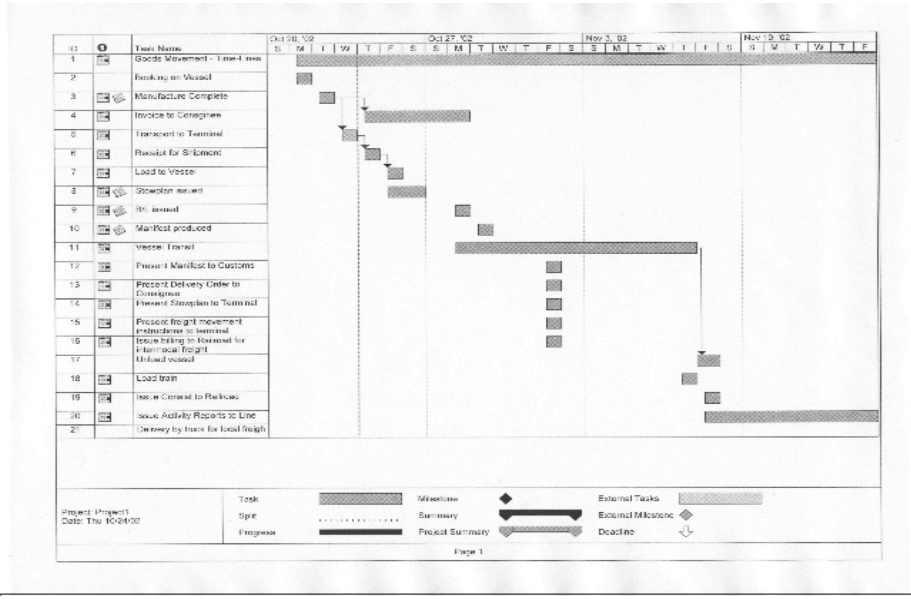
- **Contract (ramp) rail:** vessel to on-dock transfer zone to double stack rail cars for dedicated intermodal train movement at intermodal rail facility to inland destination

Daily rail: vessel to on-dock transfer zone to double stack rail car, via switching or dray to intermodal rail transfer facility to inland destination

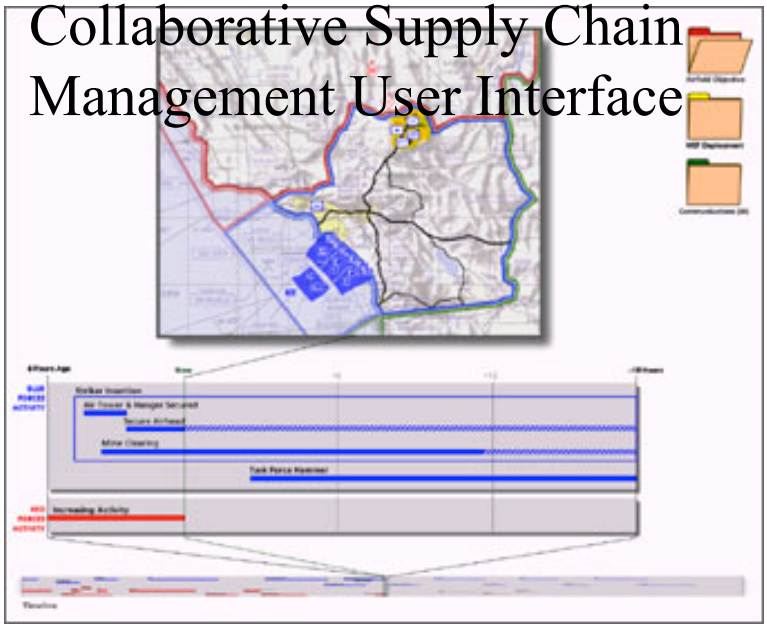
- **Trans-loading**: vessel to on-dock intermodal buffer zone and local dray to inland warehouse via OTR truck or domestic intermodal TOFC to inland destination
- **Premounted mini-bridge**: hot hatch vessel to chassis and then via local dray to local consignee
- **Store-door**: vessel to on-dock buffer zone and CFS via local dray to local consignee

Military: unit deployment via truck convoy and 89-foot flatcar to local break bulk terminal and sustainment through containerized movement

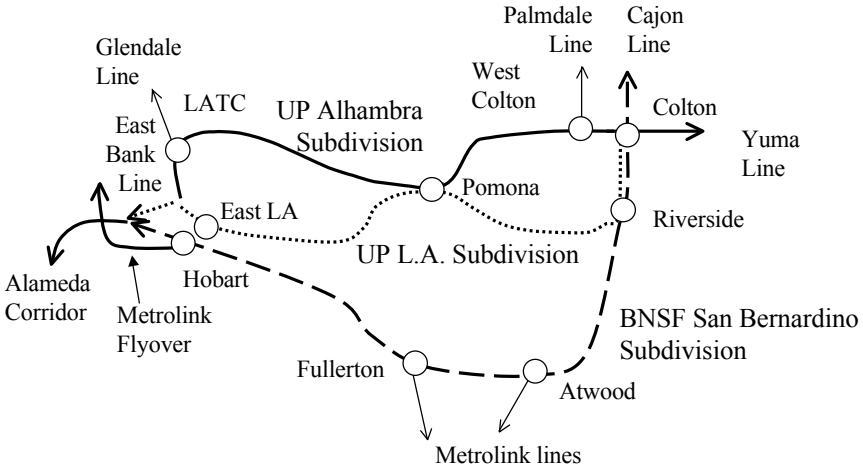
Benchmarking standard transit times for freight flows: On Dock Rail

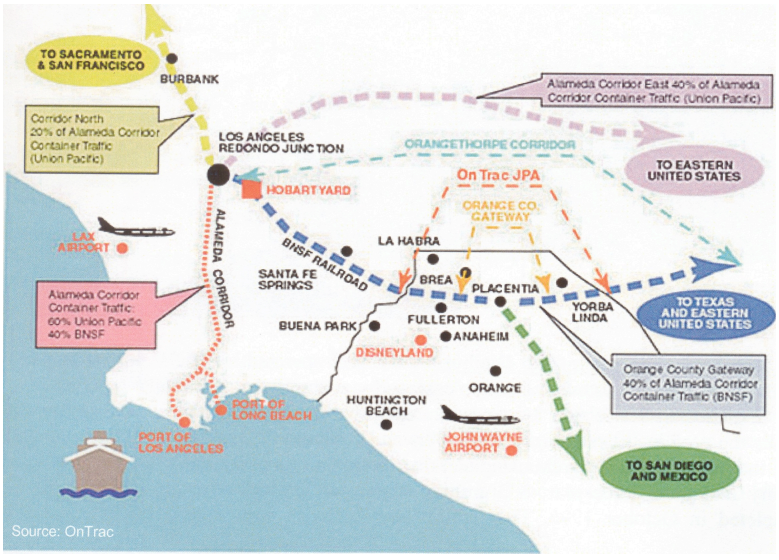


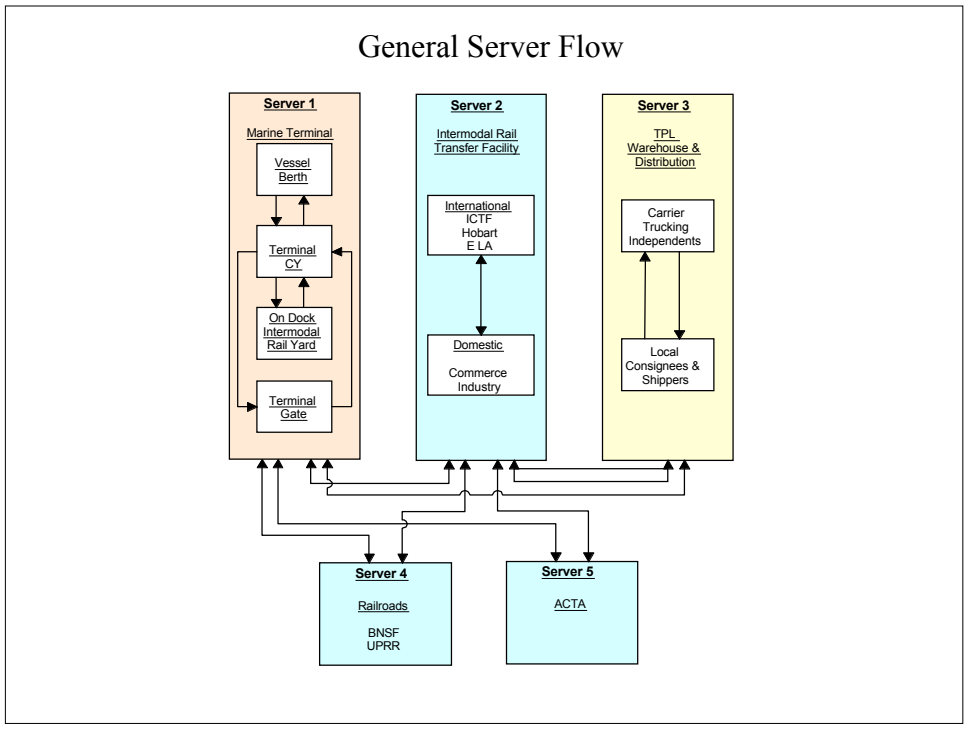
Collaborative Supply Chain Management User Interface

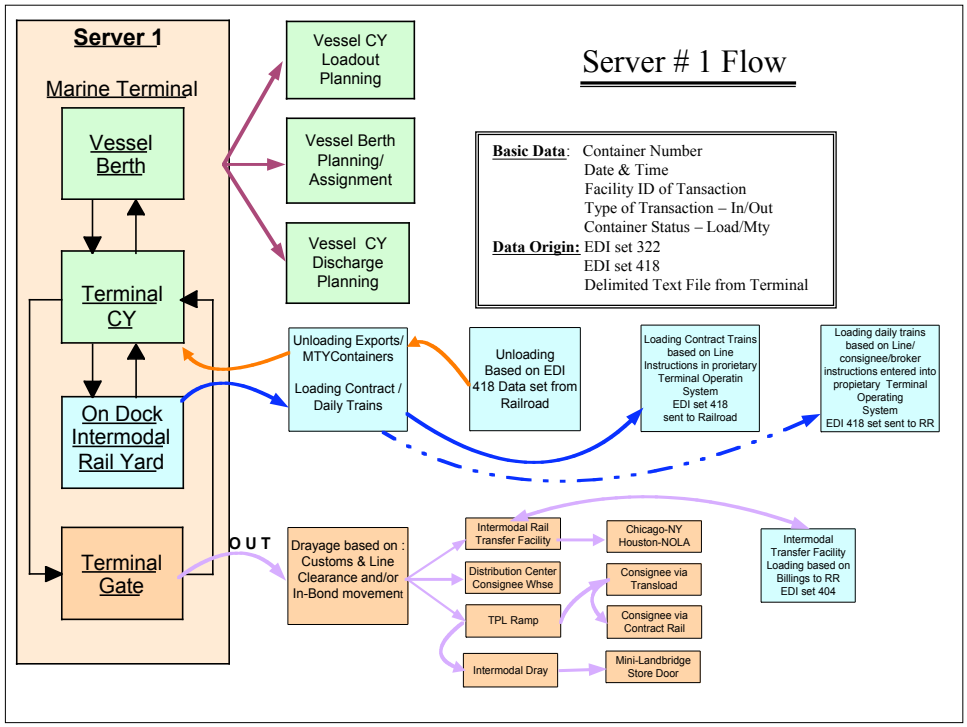


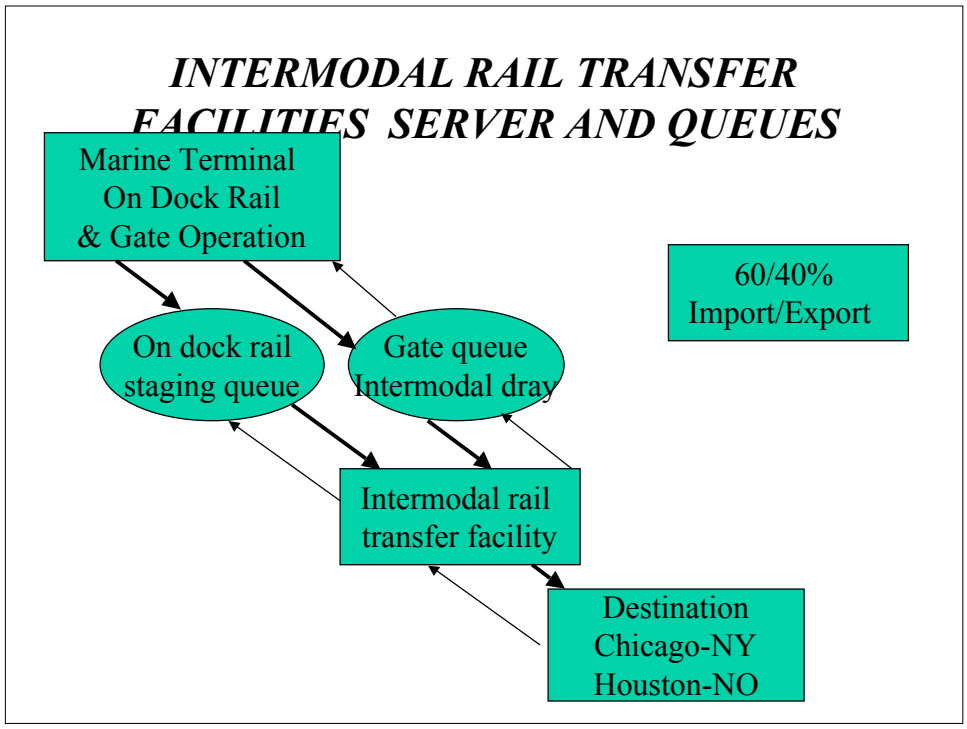
The Mainline Rail Network

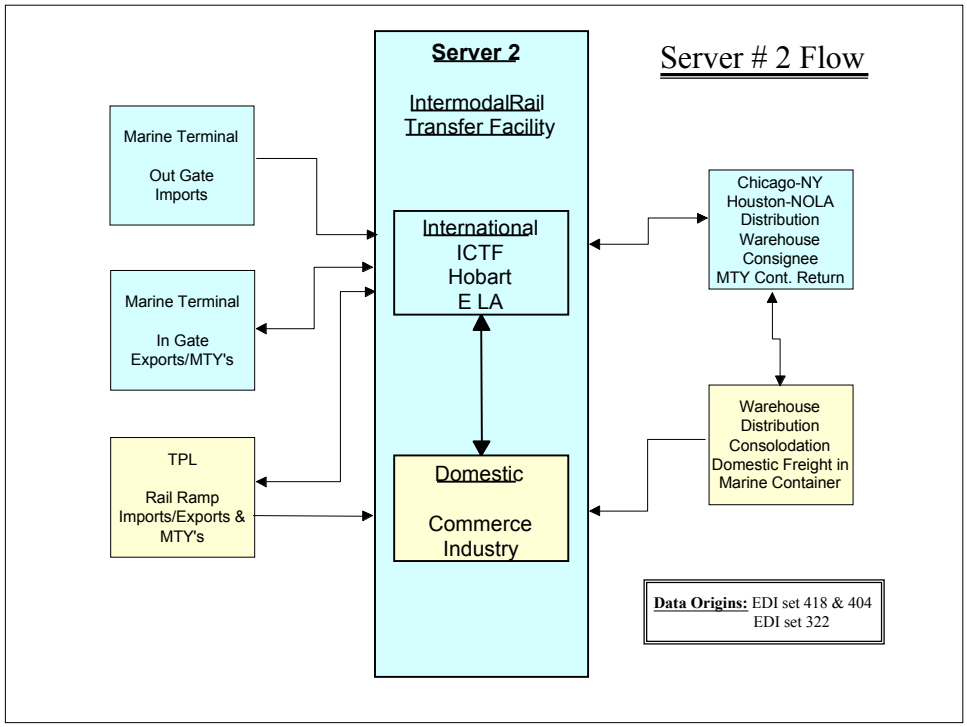


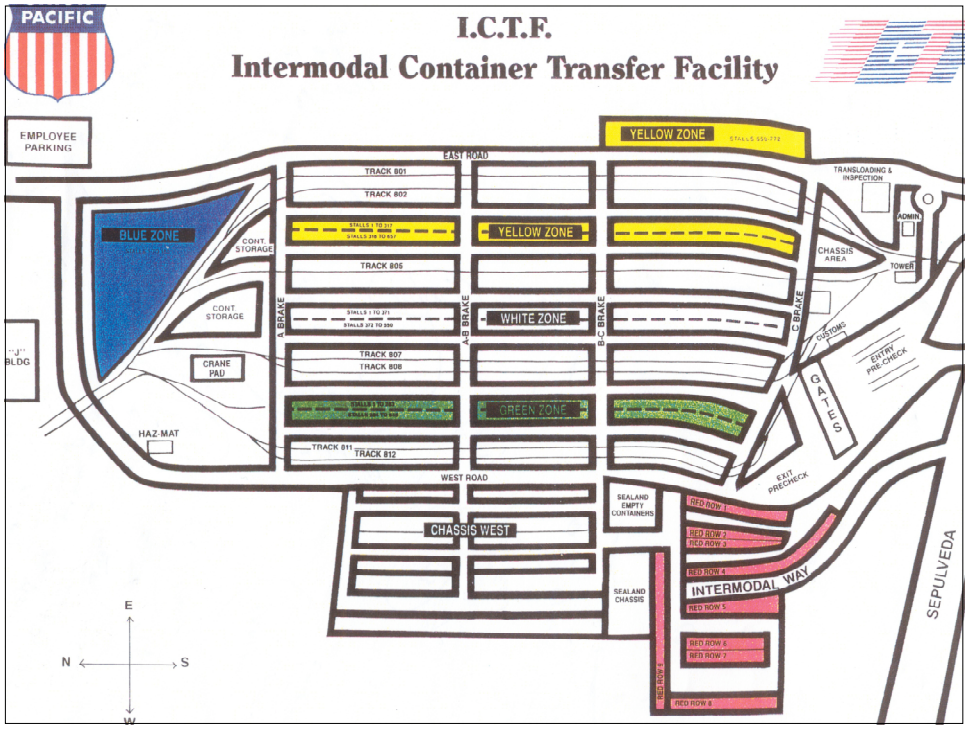



General Server Flow
Server 1
Marine Terminal
Vessel Berth
Terminal CY
On Dock Intermodal Rail Yard
Terminal Gate
Server 2
Intermodal Rail Transfer Facility
International ICTF Hobart E LA
Domestic
Commerce Industry
Server 3
TPL Warehouse & Distribution
Carrier Trucking Independents
Local Consignees & Shippers
Server 4
Railroads
BNSF UPRR
Server 5
ACTA

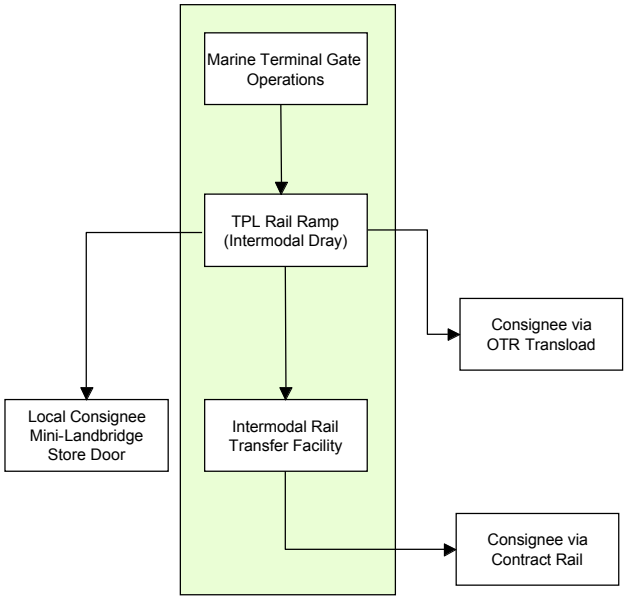

Server 1
Marine Terminal
Vessel Berth
Terminal CY
On Dock Intermodal Rail Yard
Terminal Gate
Server # 1 Flow
Vessel CY Loadout Planning
Vessel Berth Planning/ Assignment
Vessel CY Discharge Planning
Basic Data: Container Number
Date & Time
Facility ID of Tansaction
Type of Transaction – In/Out
Container Status – Load/Mty
Data Origin: EDI set 322
EDI set 418
Delimited Text File from Terminal
Unloading Exports/ MTYContainers
Loading Contract / Daily Trains
Unloading Based on EDI 418 Data set from Railroad
Loading Contract Trains based on Line Instructions in proprietary Terminal Operatin System EDI set 418 sent to Railroad
Loading daily trains based on Line/ consignee/broker instructions entered into propietary Terminal Operating System EDI 418 set sent to RR
OUT
Drayage based on : Customs & Line Clearance and/or In-Bond movement
Intermodal Rail Transfer Facility
Distribution Center Consignee Whse
TPL Ramp
Intermodal Dray
Chicago-NY Houston-NOLA
Consignee via Transload
Consignee via Contract Rail
Mini-Landbridge Store Door
Intermodal Transfer Facility Loading based on Billings to RR EDI set 404


INTERMODAL RAIL TRANSFER FACILITIES SERVER AND QUEUES
Marine Terminal On Dock Rail & Gate Operation
60/40% Import/Export
On dock rail staging queue
Gate queue Intermodal dray
Intermodal rail transfer facility
Destination Chicago-NY Houston-NO

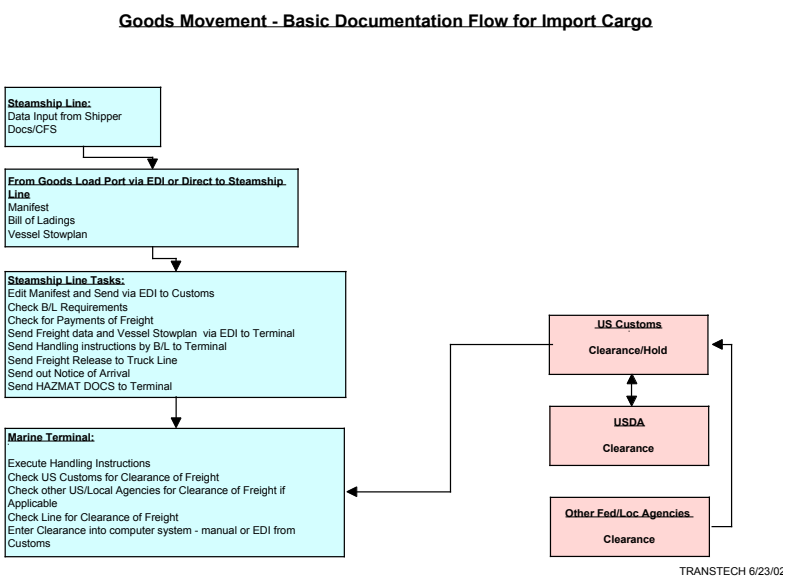

Server 2
IntermodalRail Transfer Facility
Server # 2 Flow
Marine Terminal Out Gate Imports
Marine Terminal In Gate Exports/MTY's
TPL Rail Ramp Imports/Exports & MTY's
International ICTF Hobart E LA
Domestic Commerce Industry
Chicago-NY Houston-NOLA Distribution Warehouse Consignee MTY Cont. Return
Warehouse Distribution Consolodation Domestic Freight in Marine Container
Data Origins: EDI set 418 & 404 EDI set 322

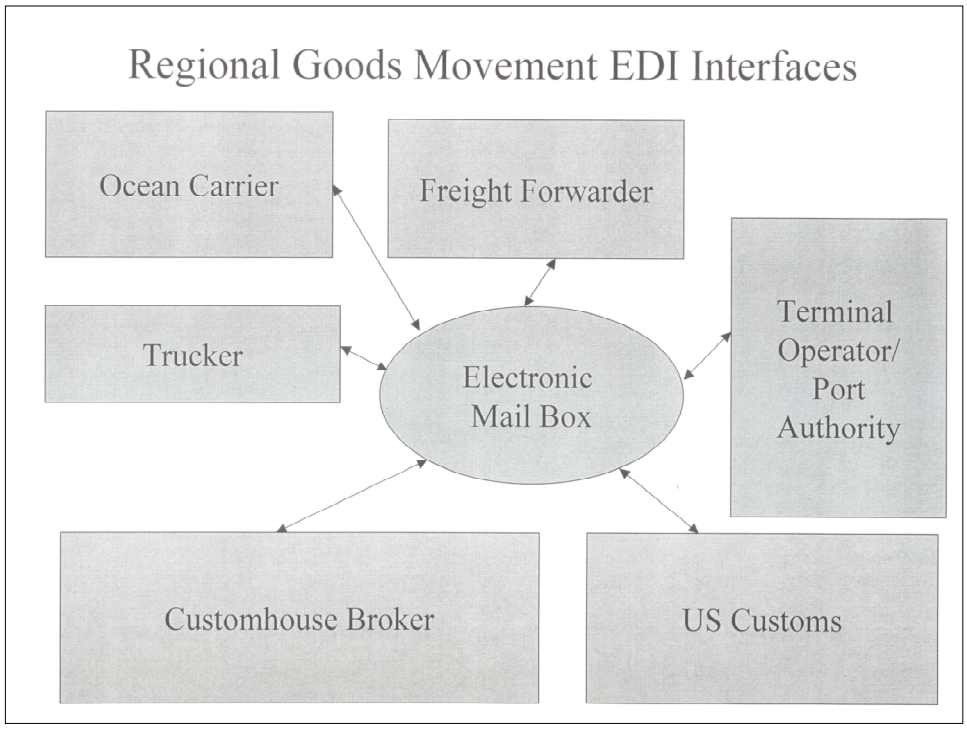


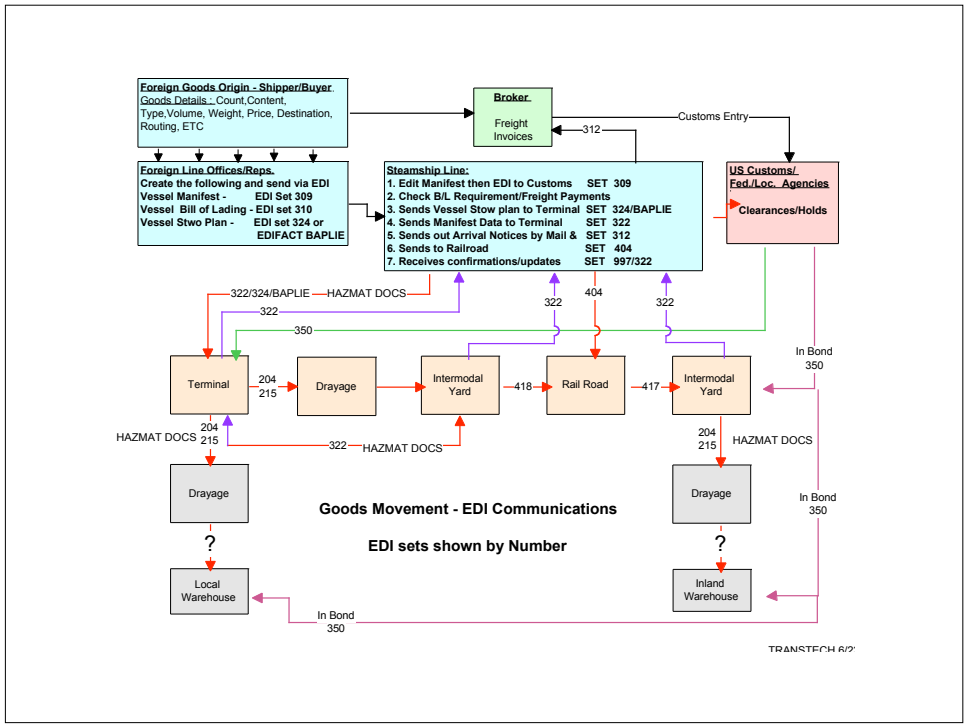
TPL Warehouse and Distribution Servers

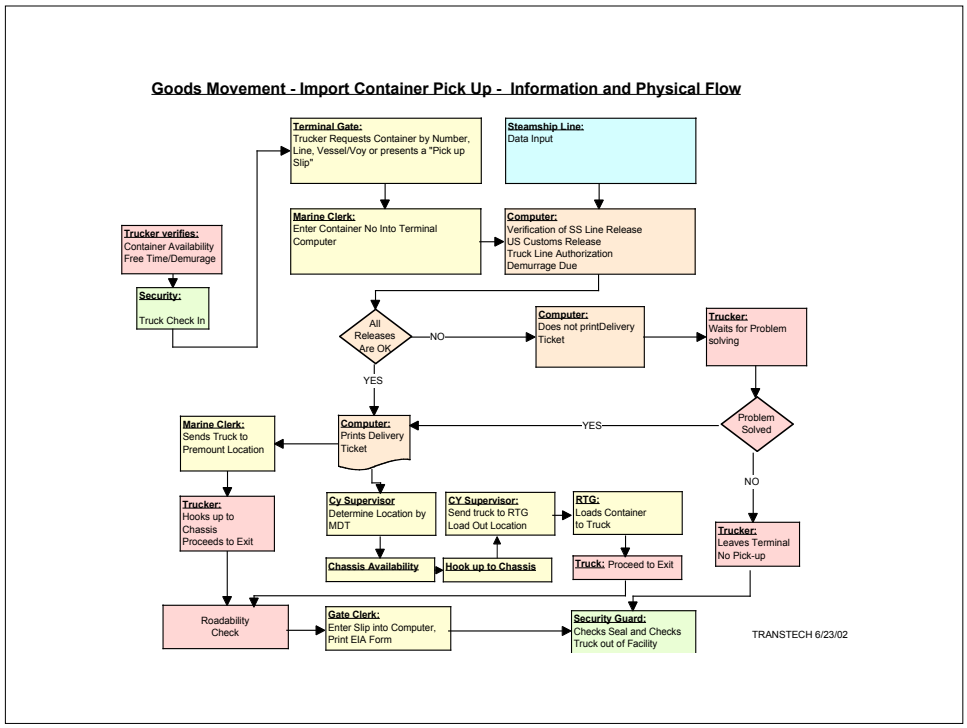


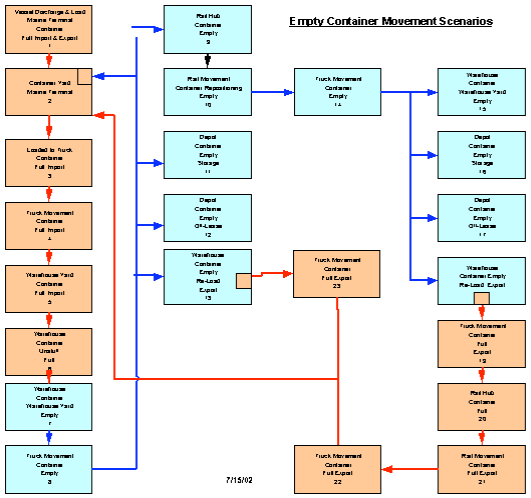
Regional Goods Movement Database built upon common data elements: container number, date/time, location origin/destination, status (empty/full) and across standard EDI transaction data sets




Regional Goods Movement EDI Interfaces
Ocean Carrier
Freight Forwarder
Trucker
Electronic Mail Box
Terminal Operator/ Port Authority
Customhouse Broker
US Customs


Foreign Goods Origin - Shipper/Buyer
Goods Details :- Count,Content, Type,Volume, Weight, Price, Destination, Routing, ETC
Broker
Freight Invoices
312
Customs Entry
Foreign Line Offices/Reps.
Create the following and send via EDI
Vessel Manifest - EDI Set 309
Vessel Bill of Lading - EDI set 310
Vessel Stwo Plan - EDI set 324 or EDIFACT BAPLIE
Steamship Line:
1. Edit Manifest then EDI to Customs SET 309
2. Check B/L Requirement/Freight Payments
3. Sends Vessel Stow plan to Terminal SET 324/BAPLIE
4. Sends Manifest Data to Terminal SET 322
5. Sends out Arrival Notices by Mail & SET 312
6. Sends to Railroad SET 404
7. Receives confirmations/updates SET 997/322
US Customs/ Fed./Loc. Agencies
Clearances/Holds
322/324/BAPLIE
HAZMAT DOCS
322
350
322
404
322
Terminal
204
215
Drayage
Intermodal Yard
418
Rail Road
417
Intermodal Yard
In Bond
350
HAZMAT DOCS
204
215
322
HAZMAT DOCS
204
215
HAZMAT DOCS
Drayage
Drayage
In Bond
350
?
?
Goods Movement - EDI Communications
EDI sets shown by Number
Local Warehouse
Inland Warehouse
In Bond
350
TRANSTECH 6/2


Goods Movement - Import Container Pick Up - Information and Physical Flow
Terminal Gate:
Trucker Requests Container by Number, Line, Vessel/Voy or presents a "Pick up Slip"
Steamship Line:
Data Input
Marine Clerk:
Enter Container No Into Terminal Computer
Computer:
Verification of SS Line Release
US Customs Release
Truck Line Authorization
Demurrage Due
Trucker verifies:
Container Availability
Free Time/Demurage
Security:
Truck Check In
All Releases Are OK
NO
YES
Computer:
Does not printDelivery Ticket
Trucker:
Waits for Problem solving
Problem Solved
YES
NO
Computer:
Prints Delivery Ticket
Marine Clerk:
Sends Truck to Premount Location
Trucker:
Hooks up to Chassis
Proceeds to Exit
Cy Supervisor
Determine Location by MDT
CY Supervisor:
Send truck to RTG
Load Out Location
RTG:
Loads Container to Truck
Trucker:
Leaves Terminal
No Pick-up
Chassis Availability
Hook up to Chassis
Truck: Proceed to Exit
Roadability Check
Gate Clerk:
Enter Slip into Computer, Print EIA Form
Security Guard:
Checks Seal and Checks Truck out of Facility
TRANSTECH 6/23/02


Empty Container Movement Scenarios
7/15/02

Military and Commercial Customer Driven Requirements

Stakeholder Collaborative

Freight Data Analysis

Output Requirements e.g Military unit deployment

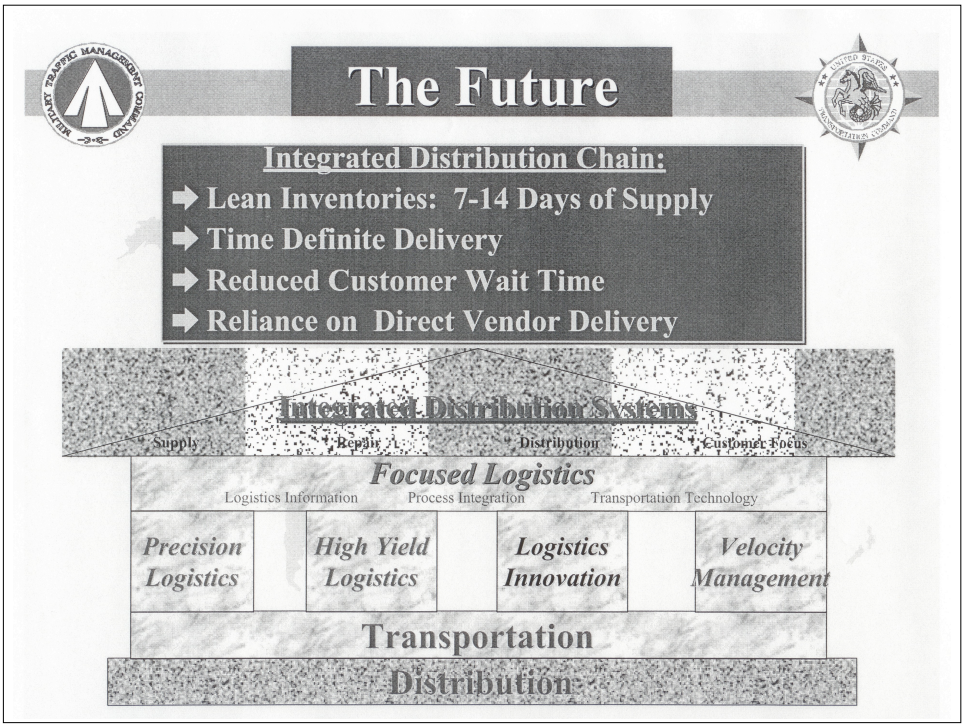
Infrastructure capacity use

Best operating practices

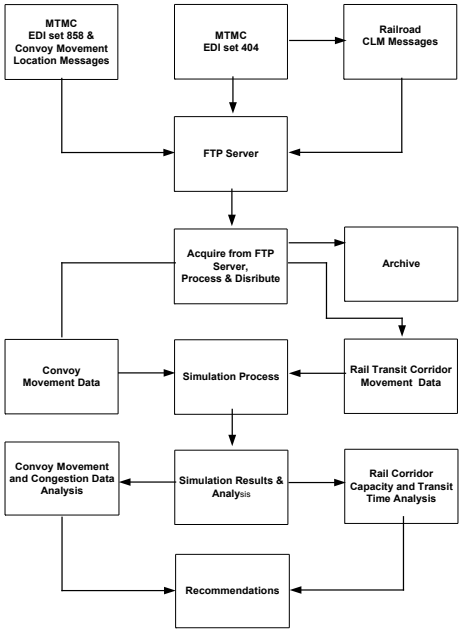
Decision Support

Public Investment

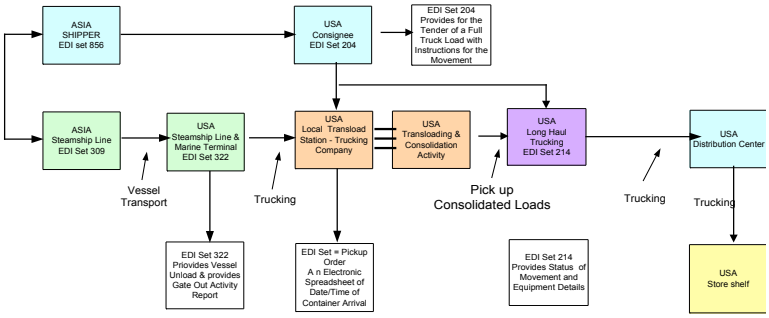
Can either be fully **Web Based** Or **Distributed Application** (Visual Basic)



EDI data Feeds from MTMC and Railroads

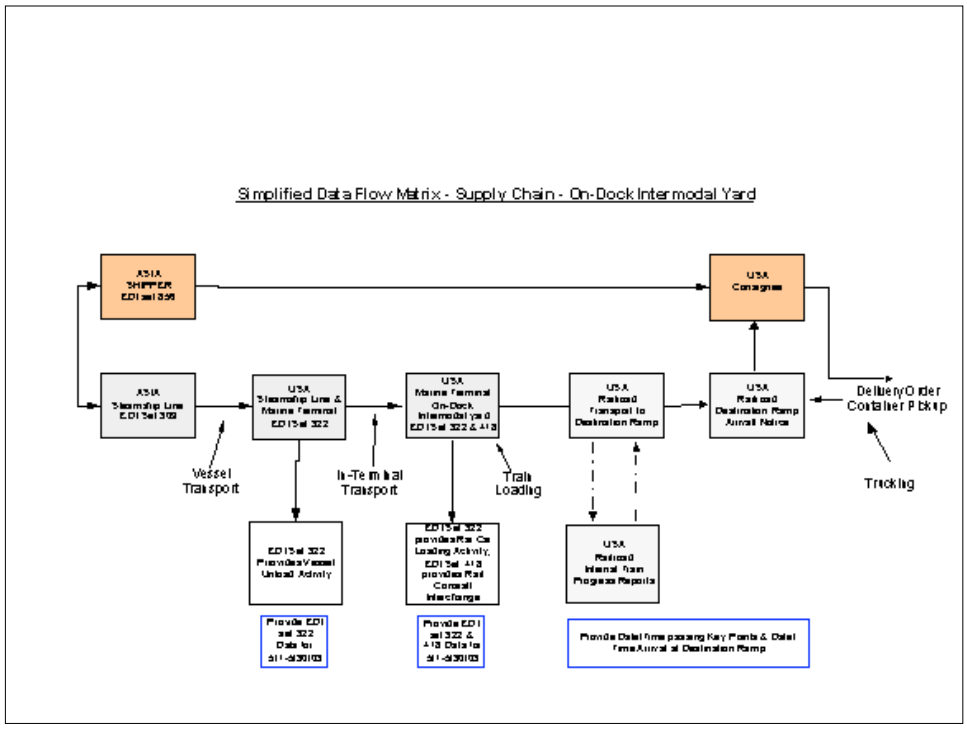


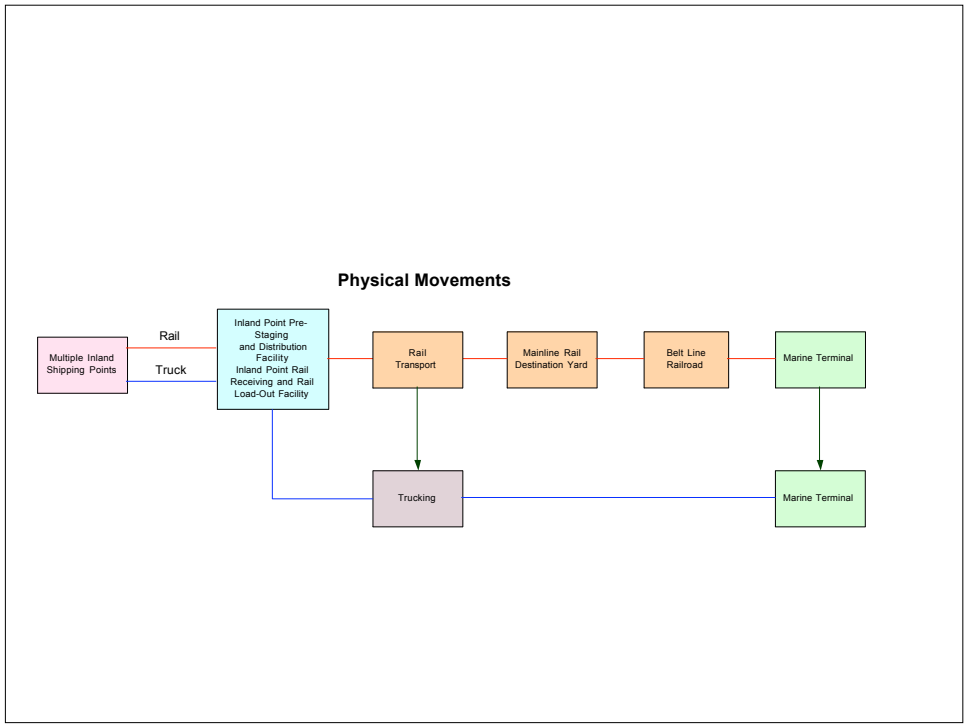
Simplified Data Flow Matrix - Supply Chain

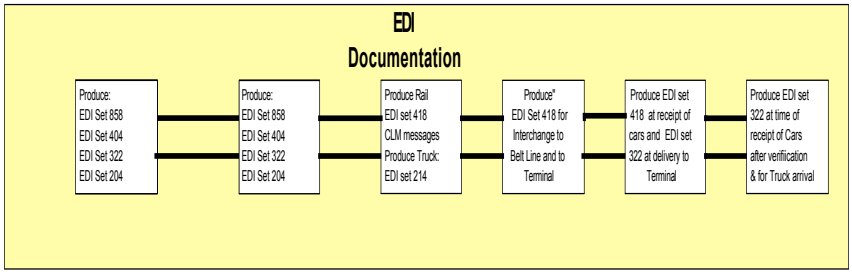


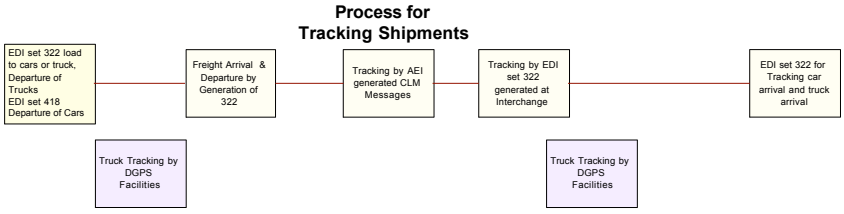
Following Data will be used from all EDI data sets:
1.Container Number
2. Date/Time of Transaction
3. Transaction Location
4. Status of Container
5. Point of Origin and Destination

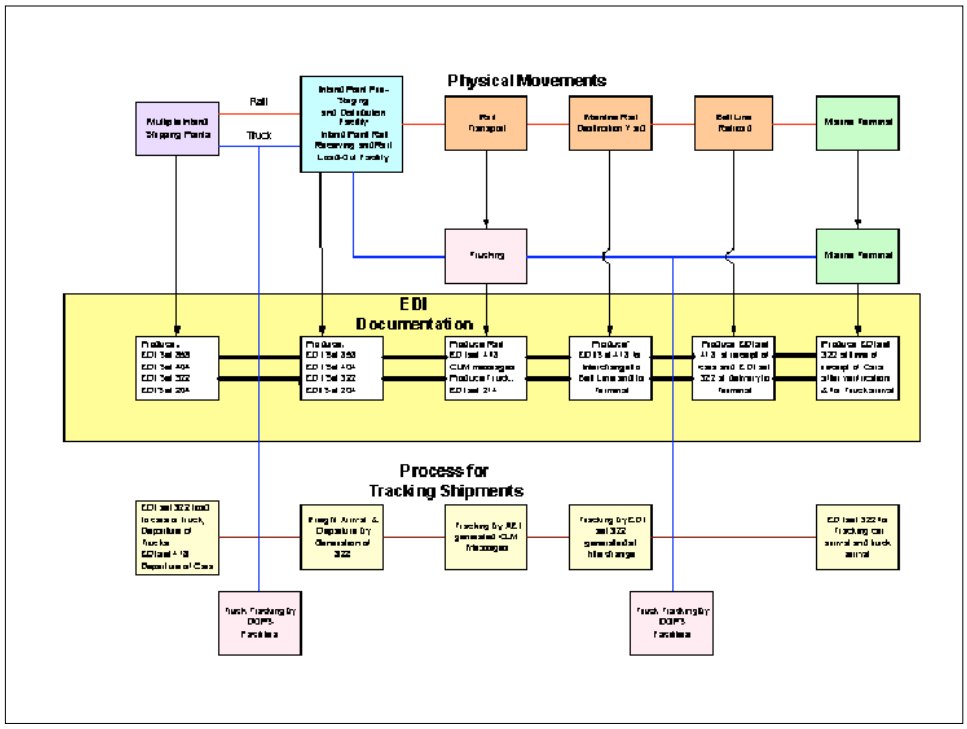
5/5/03

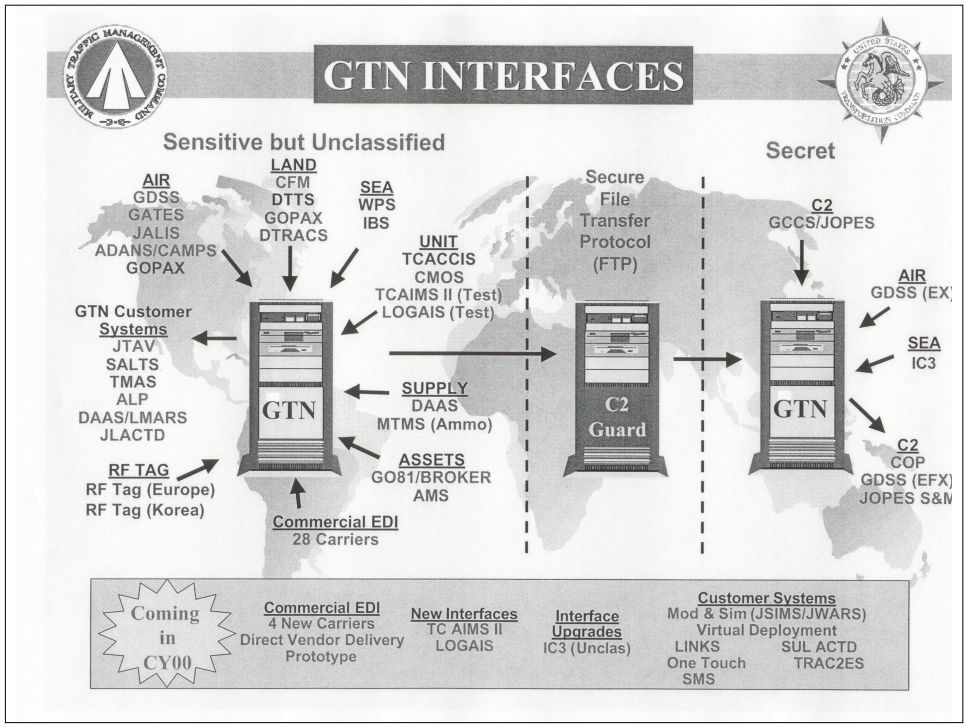

Simplified Data Flow Matrix - Supply Chain - On-Dock Intermodal Yard
ASIA SHIPPER EDI set 856
USA Consignee
ASIA Steamship Line EDI Set 300
USA Steamship Line & Marine Terminal EDI set 322
USA Marine Terminal On-Dock Intermodal yard EDI set 322 & 418
USA Railroad Transport to Destination Ramp
USA Railroad Destination Ramp Arrival Notice
Delivery Order Container Pickup
Vessel Transport
In-Terminal Transport
Train Loading
Trucking
EDI set 322 Provides Vessel Unload Activity
EDI set 322 provides Rail Car Loading Activity; EDI Set 418 provides Rail Consist Interchange
USA Railroad Internal Train Progress Reports
Provide EDI set 322 Data for 311-930103
Provide EDI set 322 & 418 Data for 311-930103
Provide Detail Info passing Key Points & Detail Time Arrival at Destination Ramp

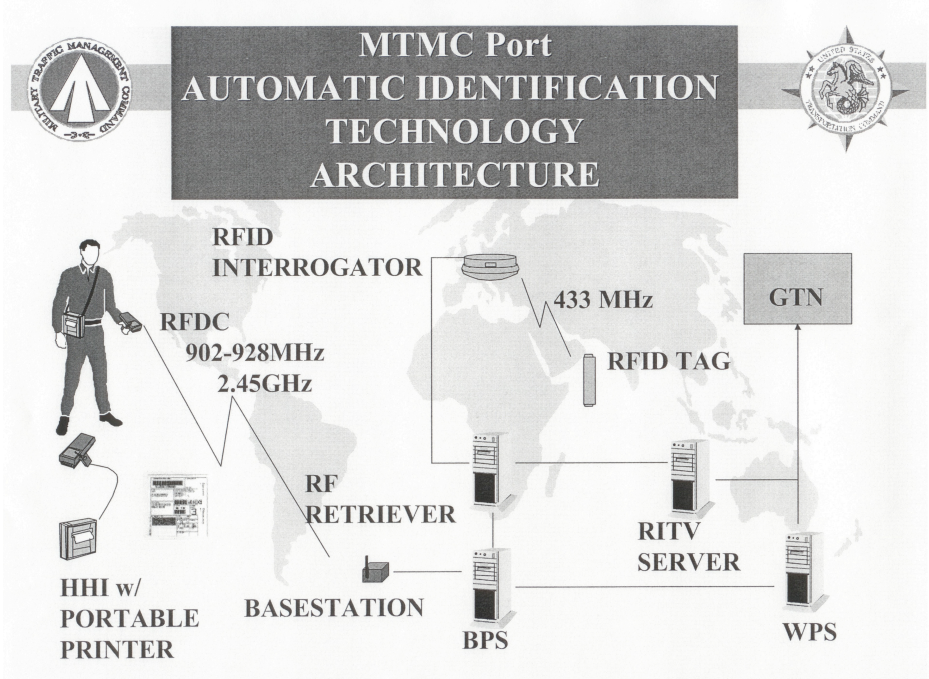

Physical Movements
Multiple Inland Shipping Points
Rail
Truck
Inland Point Pre-Staging and Distribution Facility
Inland Point Rail Receiving and Rail Load-Out Facility
Rail Transport
Mainline Rail Destination Yard
Belt Line Railroad
Marine Terminal
Trucking
Marine Terminal


EDI
Documentation
Produce:
EDI Set 858
EDI Set 404
EDI Set 322
EDI Set 204
Produce:
EDI Set 858
EDI Set 404
EDI Set 322
EDI Set 204
Produce Rail
EDI set 418
CLM messages
Produce Truck:
EDI set 214
Produce"
EDI Set 418 for
Interchange to
Belt Line and to
Terminal
Produce EDI set
418 at receipt of
cars and EDI set
322 at delivery to
Terminal
Produce EDI set
322 at time of
receipt of Cars
after verification
& for Truck arrival


Process for
Tracking Shipments
EDI set 322 load
to cars or truck,
Departure of
Trucks
EDI set 418
Departure of Cars
Freight Arrival &
Departure by
Generation of
322
Tracking by AEI
generated CLM
Messages
Tracking by EDI
set 322
generated at
Interchange
EDI set 322 for
Tracking car
arrival and truck
arrival
Truck Tracking by
DGPS
Facilities
Truck Tracking by
DGPS
Facilities


Physical Movements
Rail
Truck
Multiple Inland Shipping Points
Inland Plant Pre-Staging and Distribution Facility/ Inland Plant Rail Receiving and/Rail Load-Out Facility
Rail Transport
Maritime Port Destination Y or D
Rail Line Haul to D
Marine Terminal
Trucking
Marine Terminal
EDI Documentation
Process for Tracking Shipments


GTN INTERFACES
Sensitive but Unclassified
Secret
AIR
GDSS
GATES
JALIS
ADANS/CAMPS
GOPAX
LAND
CFM
DTTS
GOPAX
DTRACS
SEA
WPS
IBS
UNIT
TCACCIS
CMOS
TCAIMS II (Test)
LOGAIS (Test)
Secure File Transfer Protocol (FTP)
C2
GCCS/JOPES
AIR
GDSS (EX)
SEA
IC3
C2
COP
GDSS (EFX)
JOPES S&M
GTN Customer Systems
JTAV
SALTS
TMAS
ALP
DAAS/LMARS
JLACTD
GTN
SUPPLY
DAAS
MTMS (Ammo)
ASSETS
GO81/BROKER
AMS
C2 Guard
GTN
RF TAG
RF Tag (Europe)
RF Tag (Korea)
Commercial EDI
28 Carriers
Coming in CY00
Commercial EDI
4 New Carriers
Direct Vendor Delivery
Prototype
New Interfaces
TC AIMS II
LOGAIS
Interface Upgrades
IC3 (Unclas)
Customer Systems
Mod & Sim (JSIMS/JWARS)
Virtual Deployment
LINKS
SUL ACTD
One Touch
TRAC2ES
SMS



Desk Top Exercise – Model Analyses
Military Mobilization

Scenario 1. *Unit deployment* -

--1st Marine Expeditionary Force from Camp Pendleton

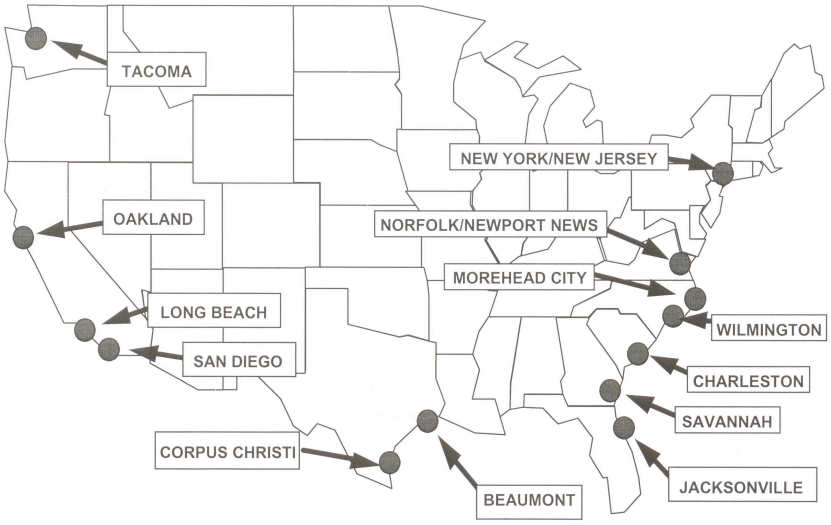
--Supply chain disruption at 38th Street Pier in San Diego

Scenario 2. *Surge deployment* –

--Sustainment by USA/USMC

--Theatre requirements determined by Defense Logistics Agency Regional Distribution Center, Tracy, CA, or HQS, New Cumberland, PA

STRATEGIC COMMERCIAL PORTS



NATIONAL PORT READINESS NETWORK

INTERAGENCY AGREEMENT

MARAD (Chair)
TRANSCOM
MTMC
MSC
USACE
USCG
MARDEZ
FORSCOM
USJFCOM

LEVELS OF COORDINATION

STEERING GROUP

WORKING GROUP

LOCAL PORT READINESS COMMITTEES

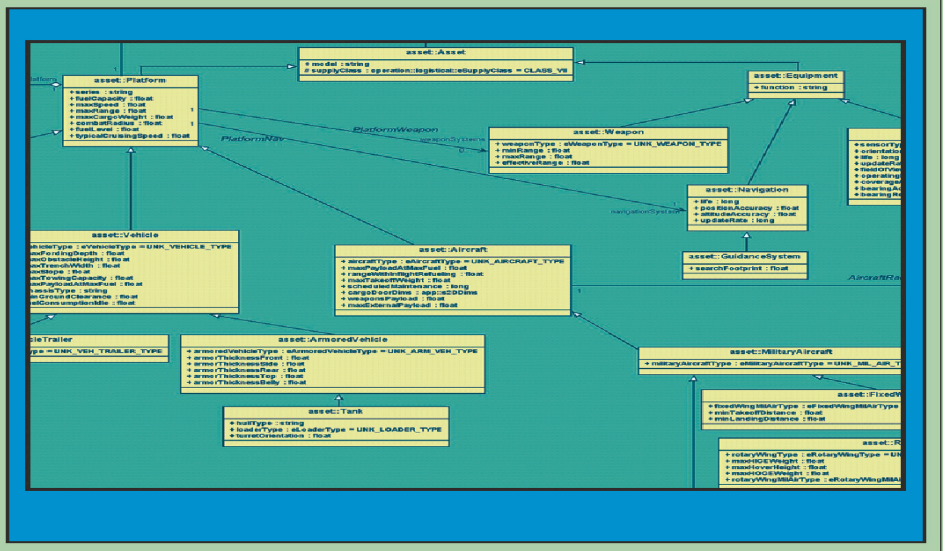
RESPONSIBILITIES

- SETS POLICY DIRECTION AND PRIORITIES
- IMPLEMENTS POLICIES AND PRIORITIES
- COORDINATES PEACETIME PREPARATION & TRAINING
- CONDUCTS PRXs
- COORDINATES PORT/CARGO SECURITY
- COORDINATES PORT OPERATIONS DURING NATIONAL EMERGENCIES

CADRC CAD Research Center

CAL POLY

Asset Domain Ontology



CADRC CAD Research Center

CAL POLY

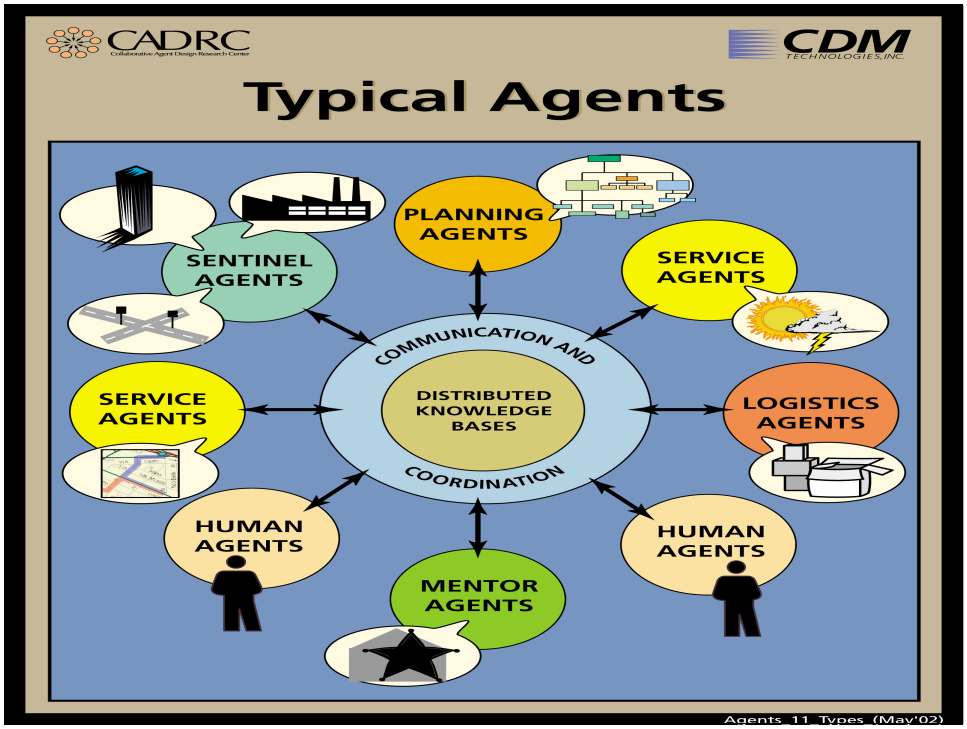
Computer-Based Agents

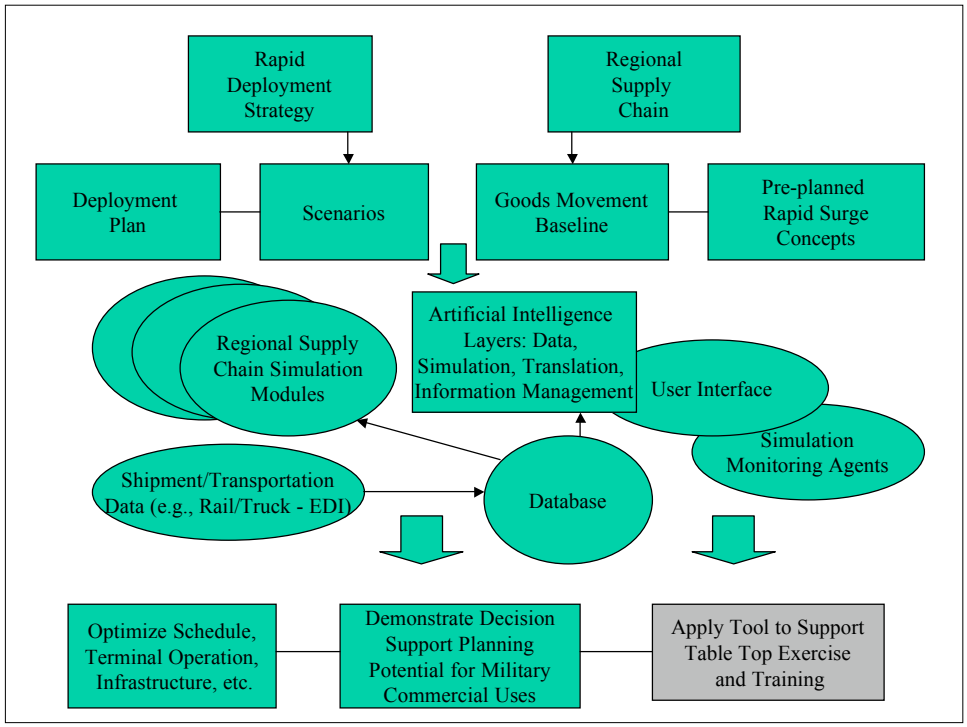
What is a computer-based agent?

"Software code that is capable of communicating with other agents to facilitate some action"

What is an intelligent agent?

1. Communicates using a common language.
2. Has *reasoning* capabilities.
3. Has knowledge and acts on its own initiative.
4. Collaborates with other agents to accomplish goals.
5. Uses local information to manage local resources.


CADRC
CDM TECHNOLOGIES, INC
Typical Agents
PLANNING AGENTS
SENTINEL AGENTS
SERVICE AGENTS
COMMUNICATION AND
DISTRIBUTED KNOWLEDGE BASES
COORDINATION
SERVICE AGENTS
LOGISTICS AGENTS
HUMAN AGENTS
HUMAN AGENTS
MENTOR AGENTS
Agents 11 Types (May'02)


Rapid Deployment Strategy
Regional Supply Chain
Deployment Plan
Scenarios
Goods Movement Baseline
Pre-planned Rapid Surge Concepts
Regional Supply Chain Simulation Modules
Artificial Intelligence Layers: Data, Simulation, Translation, Information Management
User Interface
Simulation Monitoring Agents
Shipment/Transportation Data (e.g., Rail/Truck - EDI)
Database
Optimize Schedule, Terminal Operation, Infrastructure, etc.
Demonstrate Decision Support Planning Potential for Military Commercial Uses
Apply Tool to Support Table Top Exercise and Training

CNA

Understanding Operational Collaboration in the Fleet

Sunoy Banerjee
John Bentrup
Center for Naval Analyses
Alexandria, Virginia

10 September 2003

Contact Information

- Sunoy Banerjee
  - Phone: (703)824-2064
  - DSN: 761-9638 x2064
  - E-mail: banerjes@cna.org
- John Bentrup
  - Phone: (703)824-2545
  - DSN: 761-9638 x2545
  - E-mail: bentrupj@cna.org

Outline

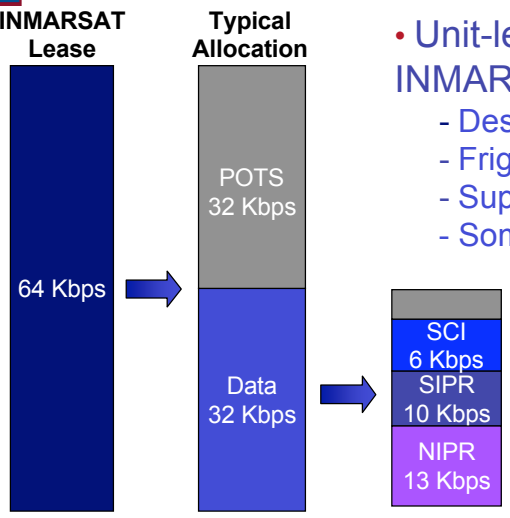
- Introduction
- At-sea environment
- Collaboration in the Navy
  - Fleet functional requirements
  - Fleet applications

Introduction: CNA projects

- 1999: Eisenhower Battle Group
  - 1st battle group wide tactical use of IRC
- 2000: Using IT for Battle Group C2
  - Project for 3rd Fleet
  - Examined appropriate use of chat
- 2001: Information Management Plan
  - Project for NETWARCOM
  - CNA study: "Proposed NETWARCOM Guidance: The Effective Use of Chat" in 2002
  - Led discussion at NCIC OAG on chat
- 2001: OEF
- 2003: Fleet IT Support
  - Project for OPNAV N61
  - CCG-1 asked CNA to look at chat issues
- 2003: OIF

At-sea environment

At-sea environment: Off-ship capacity



- Unit-level ships rely on INMARSAT
  - Destroyers
  - Frigates
  - Supply ships
  - Some cruisers

- 10 Kbps to support:
  - Individual users
  - Applications
    - E-mail
    - Web traffic

Introduction:
At-sea vs. terrestrial networks

Metric	At-sea Network	Terrestrial Network
Median Uptime	All Ships: less than 95% *CV:* __ *DD/DDG:* __ *FFG:* __	99.9%
Round-trip delay	DSCS/CWSP: 684 ms INMARSAT: 1,200 – 1,300 ms	60 ms
Capacity (per enclave)	Large-deck Ship: 200 – 384 Kbps Unit-level Ship: 10 – 50 Kbps	1,500 Kbps

Center for Naval Analyses

Introduction:
Impact on collaboration

- Ships at sea have frequent disconnects:
  - Participants regularly drop out of and must re-join chat rooms
  - Missed conversations
  - Loss of situational awareness
- Bandwidth to many Navy ships limited:
  - Difficult to support some features
    - e.g., voice, video, document sharing, etc.

COTS assumptions must be understood to ascertain product suitability for an at-sea environment

Center for Naval Analyses

Collaboration

Collaboration: Tactical vs. Planning

- Different features:
  - Text-based chat
  - File transfer
  - White boarding
  - Document sharing
  - Voice
  - Video

→ Tactical coordination
- Involves all ships
- INMARSAT-equipped ships have limited bandwidth

→ Planning
- Primarily between large deck ships and shore-based organizations
- Large deck ships have sufficient bandwidth to support additional functionality

Navy needs two different types of collaborative tools!

Collaboration:
Fleet functional requirements

"People at the bottom, the tactical level, that's the only place where mortal danger lurks, and they are the least well-connected. We're doing C4I for the admiral and the general. We have a moral obligation to fix this."

- VADM Cebrowski (Ret.)
Head of DoD Office of Force Transformation
June 2003

Collaboration:
Fleet functional requirements

- Operate at low data rates
  - Unit-level ships have roughly 10 Kbps per enclave
  - Must support tactical apps, e-mail, web traffic, AND chat/collaborative apps
- Participate in multiple rooms
  - Tactical users treat like different radio circuits
- Standing rooms
  - Rooms need to remain when users disconnect
- Public rooms
  - Users need to be able to re-join rooms easily

Collaboration:
Fleet functional requirements

- Support both Unix and Windows
  - Tactical users on GCCS-M and PCs
- Time stamp and log conversations
  - Required by law to maintain a record
- Automatic download of logs on joining
  - Allows users to come up to speed quickly
- Automatic re-connect
  - Watch standers re-join rooms immediately

Collaboration:
Fleet functional requirements

- Streamlined log-in process
  - Large log-in overhead is undesirable
  - Some browser interfaces take 3 minutes
- Distributed server architecture
  - Ships will have an organic chat capability
    - Users seldom disconnect from local servers
  - Distributed architecture can support more users
    - Organizations throughout a joint task force
    - Navy organizations around the world

Collaboration: Fleet applications

Requirements	IRC	Netmeeting	Sametime
Low data rates	90 bps	2 Kbps	2 Kbps
Multiple rooms	Yes	No	Yes
Standing rooms	Yes	Depends	Yes
Public rooms	Yes	No	No
Support Windows and Unix	Yes	No HP-UX	No Unix
Time stamp and log	Yes	No	No
Download logs on joining	No	No	No
Automatic re-connect	Yes	No	Yes
Low connection overhead	Yes	Yes	No
Distributed servers	Yes	Yes	Yes

Collaboration: Why is IRC chat so successful?

- Multi-platform support
  - Open, industry-standard protocol
  - RFC 2810,2811,2812,2813
- Operates at low data rates
  - IRC: 90 bps/user
  - Netmeeting: 2 Kbps/user
  - Sametime: 2 Kbps/user
- Supports multiple rooms
  - Chat is being used like a radio with similar guarding requirements
- Ease of use
  - On-the-job training is sufficient for IRC
- Scalability
  - No licensing issues
  - Low data rate per user
  - IRC supported rooms with ~1,000 users in OIF
- Some insensitivity to disconnects

Understanding and Applying the Cognitive Foundation of Effective Collaboration

David F. Noble

Evidence Based Research,
Vienna, VA

Abstract

Knowledge is central to collaboration and teamwork. Teams whose members know what they need to know can work together effectively. Those that do not are prone to various kinds of predictable errors, with the type of error dependent on the type of knowledge deficiency.

Our analysis of the cognitive foundations of collaboration organizes collaboration knowledge into twelve major categories. The first six of these address the mostly non-real time knowledge that team members acquire as they organize for their tasks and get to know one another over time. These are understanding team goals, the plan, dependencies (task and situation interaction models), each other, team business rules, and task work methods. The second six address the more dynamic knowledge needed to carry out the team work. These are understanding what others are doing, the external situation, task progress, areas of agreement or disagreement within the team, extent that the plan will still work, and decision factors.

Three important applications of this framework are an expert system to help teams diagnose and fix collaboration problems, a methodology for objective evaluation of the contribution of new technologies and processes to effective collaboration, and a knowledge basis for allocating functions among human and computer agent members of a team.

Introduction

Collaboration and action coordination are closely coupled activities in which team members work together to produce a product or carry out an action. Collaboration focuses on the problem solving aspects of group work. It is defined here to be "the mental aspects of group problem solving for the purpose of achieving a shared understanding, making a decision, or creating a product." In contrast, action coordination refers to the synchronized actions that people take in pursuit of common goals.

Collaboration and coordinated actions can provide many benefits (Evidence Based Research, 2001). Often the biggest payoff from collaboration arises when the team is evaluating a situation, creating an intellectual product, making recommendations, or reaching a decision. Here, team members leverage each others' perspectives to generate:

- More complete and accurate views on what is happening, the reasons for these occurrences, and their possible impact on the team mission

- More and better possible actions to take in response to the situation
- More complete and accurate criteria to consider when evaluating the desirability of these actions

- More and better possible consequences of the alternatives being considered

Unfortunately, people do not always work together effectively. The team may create products that customers don't use, and individual team members may be missing deadlines or complaining about having to do others' work or having to attend meeting they feel are a waste of time.

An understanding of the knowledge basis of collaboration and teamwork can explain fundamental causes of these problems. It can describe what's occurring "under the hood" when people work together to achieve their shared understandings, make a group decision, create such intellectual products as situation assessments, plans, analyses, and recommendations, or carry out a coordinated action. This understanding has many practical benefits. This paper describes three of these: an expert system to help diagnose and fix collaboration problems, an evaluation methodology able to explain the reasons for effective and ineffective team behaviors, and an improved rationale for partitioning team functions among human and computer agents.

The Knowledge Basis of Collaboration

Our focus on team knowledge and understandings is motivated by the foundational role of knowledge when people work together, as reflected by the following fundamental tenants:

1. Knowledge is central to collaboration and teamwork. Teams whose members know what they need to know can work together effectively. Those that do not are prone to various kinds of predictable errors, with the type of error dependent on the type of knowledge deficiency (Liang, 1995)

2. Knowledge must be distributed among members of a team. Everybody does not need to know everything for a team to be effective. But every team member does need to know how to get the knowledge he or she needs. (Wegner, 1987)

3. Individuals need to know about both "taskwork" and teamwork. Taskwork knowledge is what team members need to carry out their tasks alone. Teamwork knowledge is what team members need to know to work together effectively (Canon-Bowers, 1993)

4. The collaborative dialog helps generate the needed teamwork and taskwork knowledge. Team members exchange ideas to put in place the knowledge and understandings that team members must have for the team to achieve its mission. (Argote, 2000)

Our overview diagram of collaboration mechanisms (Figure 1) emphasizes this primary importance of knowledge to collaboration. As shown in this figure, team members' knowledge and understandings support many different kinds of team activities. Figure 1 includes three of these: team set up and adjustment, group problem solving, and synchronize and act. Team set up activities usually occur earlier and "synchronize and act" later, but in most teams these

activities re-occur as long as the team continues. Thus, most teams will revisit objectives, roles, and tasks as they solve problems and act together and discover need for clarification (Katzenbach, 1993).

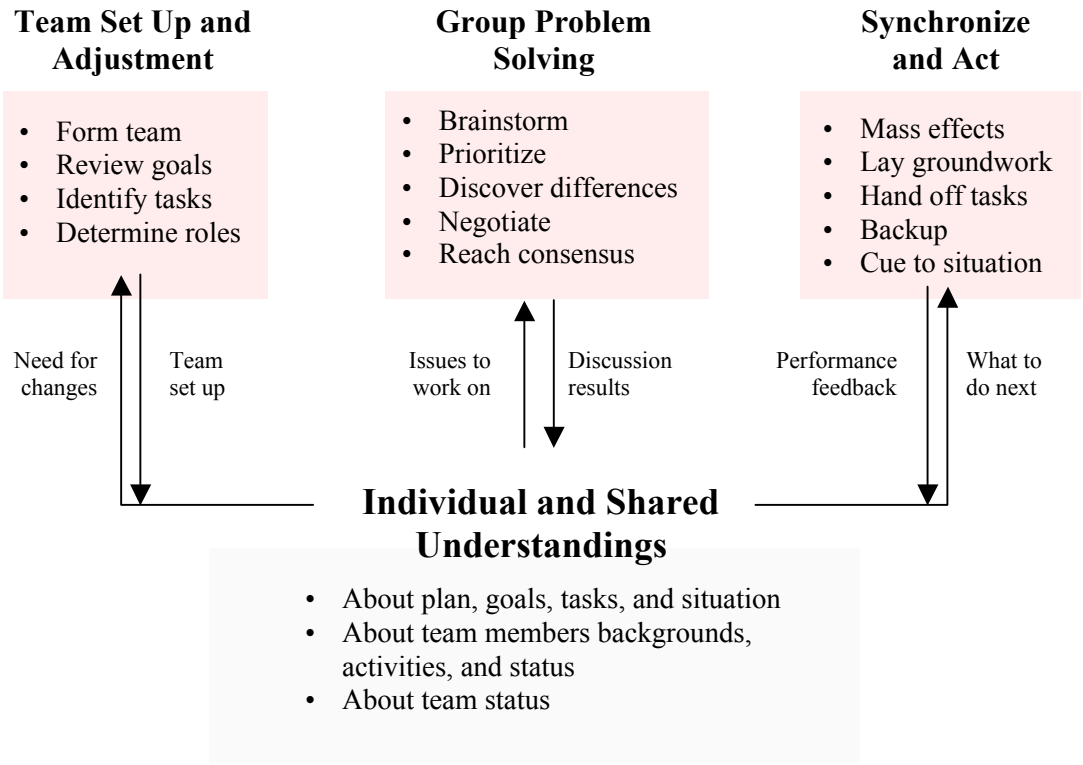


Figure 1. Building Blocks of Collaboration and Coordination

The two way arrows in Figure 1 emphasize that the knowledge both enables and is enabled by the activities in the three upper boxes. Teams cannot carry out their tasks and work together effectively if they do not have the necessary knowledge. But because teams acquire the knowledge they need to do subsequent tasks by carrying out earlier tasks, they can't acquire the knowledge they need for future tasks if they fail in earlier ones. Thus, team failure can feed on itself, with early difficulties impeding task progress, which in turn impedes obtaining the knowledge required to continue working together in future tasks.

Understanding the knowledge important to effective collaboration is the foundation to the three applications discussed later in this paper. This understanding provides the organizing principle for the Collaboration Advisor Tool that diagnoses collaboration problems and suggests remedies, provides the framework for creating a cause-effect audit trail when evaluating the impact of new technologies, processes, or organizations on collaboration, and motivates the partition of functions among human and computer agents.

Our analysis of the cognitive foundations for collaboration has organized collaboration knowledge into twelve major categories, our "knowledge enablers." This organization draws on case analyses of collaboration problems, on the collaboration research literature, and on theories of situation understanding, decision making, and command and control. We also use this

categorization because it maps easily into the different classes of commonly observed collaboration problems.

The following briefly describes each of these categories. The first six of these address the mostly non-real time knowledge that team members acquire as they organize for their tasks and get to know one another over time. This knowledge changes relatively slowly over time. The second six categories are the time sensitive understandings of team and task status and prospects at each instant of time. These understandings can change rapidly.

1. **Goal understanding** encompasses understanding team mission, the goals of the client, the criteria for evaluating team success and achievement of commander goals, and the criteria for evaluating task progress. Understanding of team objectives includes understanding both the explicit and implied goals of the team, taking into account the cultural norms of the tasking authority.

2. **Understanding of roles, tasks, and schedule** is the "surface" understanding of the plan. Project plans usually decompose the team's work into separate tasks, assign these tasks to individuals or groups of people, and then specify a schedule. The plans may specify team member responsibilities, to include both fixed and context dependent leadership roles, principal task performers, and task backups.

3. **Understanding of relationships and dependencies** is the "deeper" understanding required to project what may happen and make adjustments between tasks, resources, time, information, and the situation. The dependencies important to understand are the temporal, spatial, and causal (logical) relationships between separate tasks and between tasks and goals, information, resources, and the external situation.

4. **Understanding of team members' backgrounds and capabilities** ("familiarity" in Table 2) includes knowing other team members' values/decision criteria, to predict what they will decide; mental models, to predict what they will project; motivation, to predict their level of interest and engagement; capabilities and knowledge, to understand what they can do.

5. **Understanding of team "business rules"** includes both formal and unspoken rules by which team members work together. These are the rules for talking, listening, brainstorming, and hearing outside perspectives at meetings; (2) critiquing and editing; (3) offering/asking for help and information, (4) providing performance feedback, (5) setting up meetings (how to schedule, who to invite), (6) and cc'ing and broadcasting.

6. **Task knowledge** is the knowledge team members need to do their individual tasks. No matter how effective their teamwork is, teams cannot be successful if the individual team members lack the skills and knowledge to carry out their parts of the job. Task knowledge includes knowing how to perform assigned tasks, how to find and access documented information, how to use support tools, and how to find and access people with needed knowledge.

7. **Activity awareness** is knowing what others are doing, how busy others are, their level of

engagement, if they are getting behind or over their heads, and if they need help with their workload.

8. **Understanding of the external situation** is appreciation of everything outside of the team that can impact its work. In military operations it includes the actions of the adversary. In business it may include the actions of competitors and the preferences of customers. Understanding the external situation includes knowing who the significant players are and knowing their status, capabilities, strengths, weaknesses, behaviors, objectives, and plans.

9. **Task assessment** is determination of what tasks are being worked on and by whom, the status of these tasks, comparison of this status with the status called for by the plan, and judgment of the adequacy of available information and resources. It includes an assessment of progress and prospects for task success, including an estimate of whether a task needs help and an estimate of whether required resources and information are available.

10. **Mutual understanding** addresses the extent to which team members know how well they understand each other. It includes the extent to which team members are aware of where and why they agree or disagree about team goals, team progress, the external situation, and all the other team knowledge enablers.

11. **Plan assessment** is an estimate of whether the current team, processes, plans, and resources will still enable the team to achieve its objectives. It builds on and integrates assessments of team activities, task progress, the external situation, and degree of mutual understanding. Unlike a task assessment, which focuses on how well individual tasks are progressing, plan assessment considers all current factors and projections into the future to estimate the need for plan adjustments.

12. **Understanding of decision drivers** includes grasping all of the factors that must be considered when making a decision. These include knowing what can impact the effectiveness of a decision, and also knowing the factors that constrain the decision or can impact how the decision should be made. These include understanding the extent that a change in plan will confuse or disorient others; appreciation of appropriate decision strategy/ e.g., RPD, deliberative (Zsambok, 1993), insights into methods for handling uncertainty; and knowledge of time available and of decision trigger points/events.

Application 1: Collaboration Advisor Tool

The Collaboration Advisor Tool is a team self-help diagnosis and recommendation expert system. It diagnoses the underlying reasons for team difficulties in terms of the twelve knowledge enablers, lists warning signs for future problems in the knowledge areas of greatest concern, and suggests processes and tools to alleviate these problems. It also provides a "team view" to summarize and compare team member perspectives.

Diagnosis. Figure 2 is an overview of the tool's logical structure for diagnosing knowledge inadequacies. The four blocks at the top represent the product development flow, from

information to team knowledge, to team behaviors, and to products. The bottom set of blocks are the issues the collaboration advisor tool considers when making its diagnoses. These are knowledge risks, knowledge importance multipliers, and behavioral symptoms of knowledge problems.

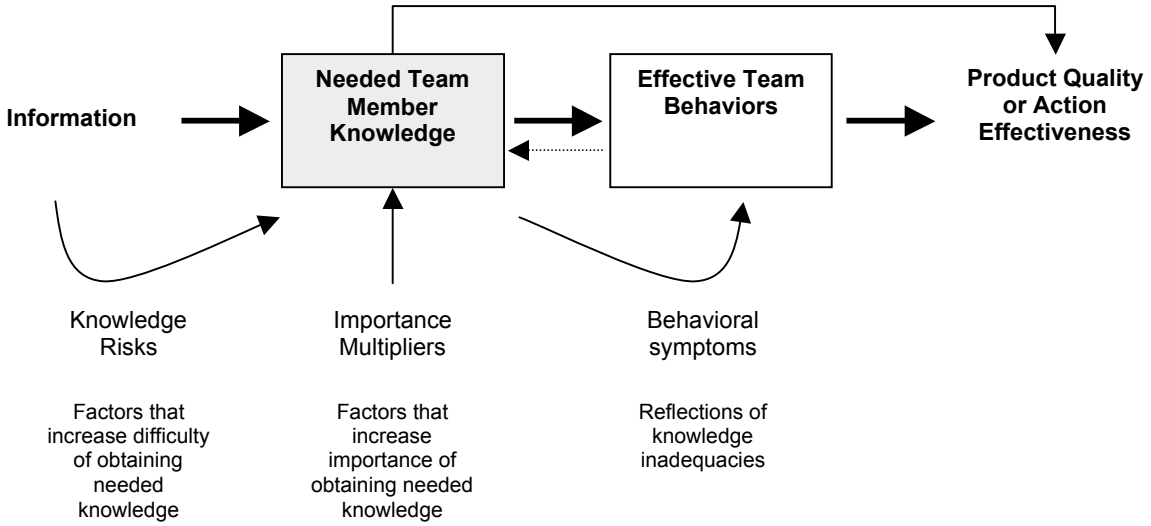


Figure 2. Factors Impacting Collaboration Advisor Diagnoses

The tool knowledge base has separate sections for diagnosis and for remedy suggestions. Table 2 illustrates some of the knowledge risks, importance multipliers, and behavioral symptoms useful in diagnosing team problems in goal understanding.

The knowledge base has similar entries for each of the twelve knowledge enablers. Because a risk, multiplier, or symptom usually applies to more than a single enabler knowledge category, the tool uses evidential reasoning in diagnosing team problems and assigning a level of concern for each of the knowledge areas. For example, in assigning a level of concern for a risk, the advisor tool considers the degree of risk a particular issue imposes for each of the knowledge areas, the number of knowledge areas it impacts, and the overall level of current concern for each knowledge area it can affect.

Advisor remedy suggestions. Once it makes its diagnosis, the advisor tool suggests remedies for team areas of concern. It makes a "canned" suggestion for each of the enabler areas, and makes additional specific recommendations for issues that the tool identifies as significant.

As an example, the general advice for concerns about team goal understanding is:

> "The most direct way to understand explicit team goals are briefings and documents stating these goals, as in written plans and requirements traceability documents. Interactions with leaders (e.g., military commanders) and clients help convey both explicit and implicit goals, especially when non-verbal cues may be communicated. Knowing the leaders, clients, and their cultures helps people understand implicit goals. Group discussions of specific success criteria, especially in terms of the properties of

desired team products, contribute to goal understanding."

Knowledge Base Category	Examples of Knowledge Base Elements
Risks: Makes obtaining needed knowledge more difficult	Customer goals and expectations are not clearly stated The team has multiple competing/conflicting goals Some team members are unfamiliar with a customer's business area or culture Criteria for determining mission success or product quality are unclear Criteria for determining task progress or reaching milestones are unclear
Multipliers: Makes having the knowledge more important	Anomalous unanticipated situations are likely to arise Timely clarification or feedback is not readily available
Symptoms: Indicates gaps in needed knowledge	People act in ways which the leader or sponsor believe are inconsistent with intent Team members argue or disagree about what achievements constitute success Team members propose actions which if successful would be inconsistent with intent

Table 1. Illustrative Knowledge Base Entries for Diagnosing Gaps in Goal Understandings

Continuing the example, the specific suggestions that the tool makes for the risk (see Table 1) "The team has multiple competing/conflicting goals" is:

1. Identify possible obstacles or challenges to meeting plan goals
2. Analyze goal and task conflicts to determine how the conflicts can be mitigated or how goal achievement can be modified to reduce conflicts.
3. Discuss with customers, stakeholders, and team members the desirability of various possible goal trade-offs
4. Develop consensus of team members on customer requirements, goals, and expectations
5. Publish customer requirements and team consensus on goals and expectations

Team View. The collaboration advisor can collect the perspectives of team function from each team member, and then create a consolidated team view. This view points out areas of agreement and disagreement within the team, and in each area displays the number of team members with each perspective. The team view summarizes the knowledge areas, team risks, and behavioral symptoms of greatest concern.

Application 2: Collaboration Evaluation

Collaboration evaluation has two principal goals. First, it seeks to quantify changes in team performance, in order to determine the extent to which a new technology, process, or organization improves team effectiveness. Second, it seeks to explain the reasons for changes in effectiveness. The paper "Objective Metrics for Evaluation of Collaborating Teams" (Noble, 2003) and the handbook "Command Performance Assessment System" (Kirzl et al. 2003) describe methods of objectively evaluating team performance. This paper focuses on the key role of team knowledge in explaining the reasons for changes in effectiveness; e.g., in creating an impact audit trail.

An objective evaluation that quantifies the change in team performance is an important part of an evaluation. Usually, however, a sponsor desires to understand not only how much team performance is improving, but also wants to understand the reasons for the improvement. Understanding the changes to team understandings and knowledge is an important part of the improvement audit trail.

Explanatory audit trails can identify the reasons for changes in team performance. Figure 3 outlines the audit trail components: the information presentation and communication tools, the team knowledge, the team behaviors, and actions and products. The team knowledge is the contents of twelve enabler categories previously discussed. The critical behaviors measure the extent to which the team coordinates and adapts well. The audit trail framework organizes the critical team behaviors into nine categories. The first three of these concern how well the team coordinates and synchronizes its tasks. The next four categories concern how well the team manages and handles information. The last two categories address a team's ability to change when needed.

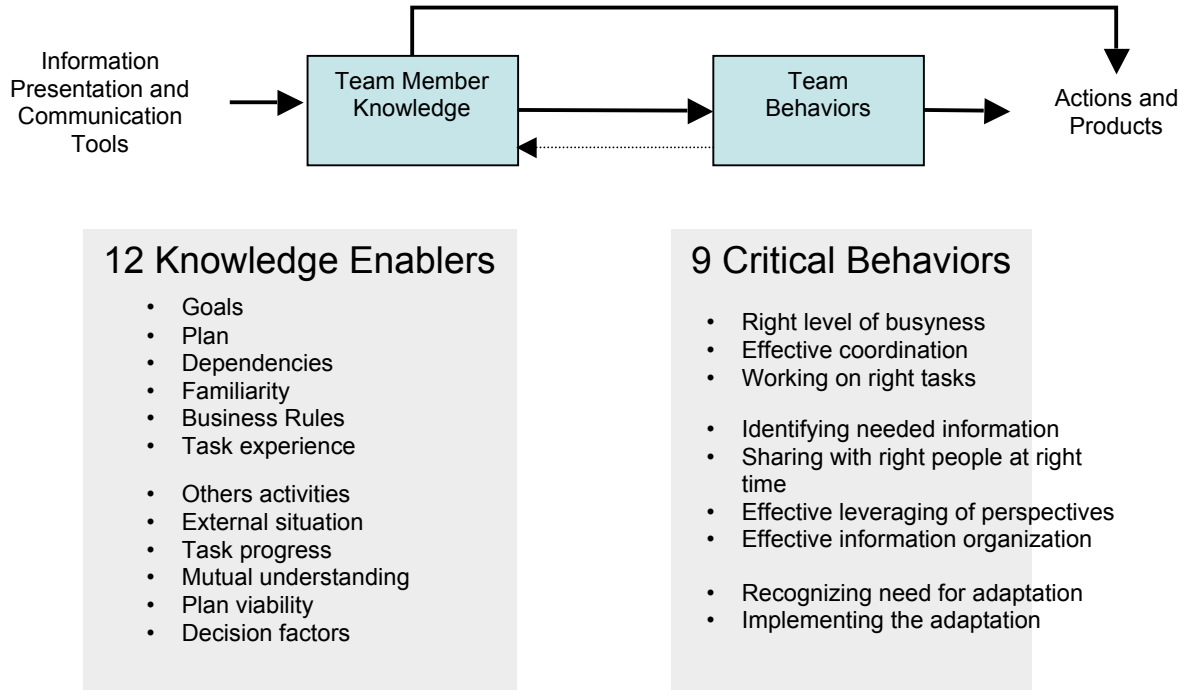


Figure 3. Elements of the Evaluation Audit Trail

This audit trail enables team evaluators to tell a causal story explaining why a new technology, process, or organization improves team performance. For example, a spatially distributed team may produce a product more efficiently when a collaboration tool that helps them be more aware of each others' activities is introduced. The overall performance metrics might show that the team is now creating a better product (as measured using the product metrics) faster and with fewer person hours. The behavioral metrics might then document that team members have reduced performing unnecessarily redundant tasks and members spend less time waiting for team members to finish precursor tasks. The knowledge metrics might document that team members are much more aware of what each other is doing, thus enabling the improved coordination. An analysis of the new information technology confirms that its displays are designed to help people know what others are working on.

In order to document this story, evaluators need to measure each of the steps in the audit trail. They need to measure the properties of the tool, process, or organization that could plausibly impact knowledge. Then they need to measure the knowledge itself to show how much it changed. Next, they need to measure the behaviors, and finally, they need to measure the products. The evaluation handbook (Kirzl et al. 2003) describes each of these steps. This paper reviews the first two steps: measurement of the environment properties that can impact knowledge, and measurement of the knowledge itself.

Risks to knowledge. As described in that handbook, the link between the supporting infrastructure (tools, processes, and organization) and knowledge are various risks to knowledge. These risks are task, team, and environmental factors that increase the difficulty of obtaining the knowledge needed for effective performance. Table 2 provides examples, selected from the more extensive set in the handbook, for how some illustrative tool and tool services can impact some knowledge risks. The left column of the table lists illustrative tool services. The middle column lists knowledge risks that the tool service reduces. The right column references one or two of the knowledge enablers affected by that risk.

Tool and Tool Service	Knowledge / Understanding Risk	Key Knowledge Areas Impacted
Applications that enable team member's input (new material, comments) in near-real time	It is difficult to see other people do their jobs	Activity Awareness
	It is difficult to link team products to the people who did them	Familiarity, Mutual Understanding
Monitors for watching others work	It is difficult to see other people do their jobs	Activity Awareness
	Team members are sometimes assigned to tasks based on title rather than skill	Task Knowledge
Monitors focusing on external situation changes	It is a difficult environment in which to discover problems early	External Situation
	There are significant time lags between taking an action and knowing the result	External Situation, Decision Drivers

	It is hard to see quickly the changes people make to either the situation or to team products	Activity Awareness, External Situation

Table 2. Example of Tools and Services that Reduce Knowledge Risks

Measuring changes to critical team knowledge. Changes to team knowledge may be measured by asking people questions that they need the knowledge to answer. Alternatively, this knowledge can be inferred from overheard team statements or behaviors. The latter is especially important in environments where team participants cannot be disturbed to answer questions.

The first method of measuring knowledge is to ask the team participants questions. The handbook suggests questions for each of the twelve knowledge categories. Example questions for "familiarity" (knowledge about others on team) are:

1. Who on the team are most knowledgeable about y?
2. Who has experience in subject y?
3. What is person z likely to think about y?
4. What is he most likely to do in situation y?
5. What are the conditions under which y is likely to need help with task z?

The second way of measuring knowledge is to infer it from overheard statements and team member behaviors. These behaviors and overheard statements are the knowledge deficiency symptoms, and are the same ones that the collaboration advisor tool uses to help diagnose gaps and deficiencies in each of the knowledge categories.

Table 3 lists five symptoms extracted from a more comprehensive table in the evaluation handbook. The first three of these were also shown in Table 1. The second column notes the data to be collected at each observed instance of a symptom. The third column scores how often the symptoms are observed, a count used to weight its significance.

Symptom	Data to be Collected	Scoring
People act in ways which the leader or sponsor believe are inconsistent with intent	Questionnaire or recorded leader feedback to staff	# of inconsistent actions per time period
Team members argue or disagree about what achievements constitute success	Recorded disagreements	# of disagreements/time period
Team members propose actions which if successful would be inconsistent with intent	Recorded actions. SME determine inconsistencies	Ratio of # of inconsistent actions to total actions
Sometimes team members pursue their own objectives rather than support team needs	Questionnaire	# of occurrences per time period

Team members state that some past team decision or orders contradicted overall intent	Questionnaire	# of occurrences

Table 3. Example of Handbook Table for Symptoms of Poor Goal Understanding

Each of the symptoms in the table can be a sign of poor understanding of goals. Unfortunately, as previously discussed with respect to the collaboration advisor tool, most symptoms are ambiguous. The fourth symptom can also imply poor understanding of the plan or relationships. The fifth can imply poor understanding of decision factors. Therefore, inference of the knowledge from symptoms requires evidential reasoning. In fact, because this is the same evidential reasoning that the collaboration advisor tool performs, that tool can be a significant support in documenting team member knowledge, and thus in creating the evaluation audit trail.

Application 3: Agent Functional Allocation

In "mixed initiative" human-computer systems, people and computers work together to solve a problem and achieve a goal. Designers of such systems are admonished to "task computers with work computers do best, and to task people with work that they do best."

Though the line between what computers do well and what people do well continues to shift as technology improves, it is agreed that today computers are best at arithmetic, data storage, data sharing, and reasoning confined to well structured problems. They can accomplish these tasks quickly and reliably. In contrast, people need to be entrusted with any task that requires "common sense reasoning" based on people's experience interacting with the world and with each other. Computers have particular difficulty when reasoning requires an understanding of societal norms, values, and conventions or when reasoning requires the computer to input from unstructured perceptional cues (interpreting a movie), such as natural language comprehension and scene interpretation.

Table 4 applies these general guidelines specifically to collaboration. It describes for each of the twelve collaboration knowledge categories those parts of the knowledge and understanding that computers address and the knowledge and understandings which given current levels of computer intelligence, should be reserved for people. Functional allocation then follows from the knowledge assignments. Functions whose success requires knowledge in the "human strength" column should be assigned to people. Those that need only knowledge in the "computer strength" column are good candidates for assignment to computers.

Knowledge Category	Computer Strength	Human Strength
Goal Understanding	Explicit goals associated with concrete measurable objectives	Goals implied by cultural norms
Understanding of roles, tasks, and schedule	Knowledge of plan and schedule, as recorded in planning documents Formally specified team roles	Knowledge of backup and default team member roles based on knowledge of team members character and past experiences Extent that a schedule can slip without violating unstated "real" goals
Understanding of relationships and dependencies	Physical relationships among entities, especially time-distance relationships	Relationships that depend on understanding human behaviors and motivation
Understanding of team members' backgrounds and capabilities	Credentials, as expressed in defined ontology Extraction of backgrounds by review of topics in documents written	Team members' values and character, as needed to predict action in unusual circumstances
Understanding of team "business rules"	Rules for informing others, for accepting edits, and enforcing formal permissions	Understanding the reasons for rules, in order to know when it's appropriate to modify
Task knowledge	Routine and standardized tasks reducible to algorithm or formula. Retrieval of documents and written information	Tasks requiring imagination and creativity Elicitation of information from people Tasks requiring understanding of implicit human values
Activity awareness	Tasks people are working on, as implied by documents they are accessing and people they are interacting with through computers	Tasks people are working on, as inferred by watching them work. Level of engagement in tasks, as inferred from body language and other non verbal cues
Understanding of the external situation	The locations and identity of situation participants, as inferred from reports	The motivations, goals and plans of situation participants, as inferred from current and past experiences
Task assessment	Task progress, as inferred from development of computer readable documents Needed resources and information, as specified in written plan	Task assessment as inferred from verbal reports and inspections of product Estimates of difficulties from non-verbal cues and familiarity with team members
Mutual awareness of team member understandings	Facts in distributed data/knowledge bases Consistency of facts, based on literal interpretations	Extent of agreement/disagreement based on behaviors and on past knowledge of people's goals, values, and behavioral styles
Plan assessment	Extent plan will work, based on recorded task progress and resource/information inventories and on formal mathematical models of task dependencies and resources	Extent plan will work based on observed or verbally reported task progress Projections that depend on forecasting human behaviors
Understanding of decision drivers	Knowledge of planned and standard actions, of schedules time available to make decision, and of specified sub-goals	Knowledge of how human team members and adversaries may react to plan changes Identification of unstated action constraints based on societal and client values

Table 4. Knowledge Most Conveniently and Reliably Allocated to People or Computers

References

Argote, L. and P. Ingram. (2000), Knowledge Transfer: A Basis for Competitive Advantage in Firms. Organizational Behavior and Human Decision Processes, Vol. 82, No. 1, (pp 150-169)

Canon-Bowers, J.A. Salas, and S. A. Converse. (1993). Shared Mental Models in Expert System Team Decision-Making. In Individual and Group Decision Making: Current Issues,

eds. M. J. Castellan. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc./

Evidence Based Research (2001), Enabling Effective Collaboration in Military Operations. Workshop Report. Evidence Based Research, Vienna, VA.

Evidence Based Research (2002], Collaboration Guidelines, Identifying and Fixing Collaboration Problems. Draft. Evidence Based Research, Vienna, VA. Katzenbach, J.R. and Smith D.K. (1993); The Discipline of Teams. Harvard Business Review, 71 (2): 111-120

Kirzl, J, Noble, D., and Leedom, D. (2003); Command Performance Assessment System. Vienna, VA: Evidence Based Research.

Liang, D., R. Moreland, and L. Argote. (1995). Group Versus Individual Training and Group Performance: The Mediating Role of Transactive Memory. Personality and Social Psychology Bulletin, Vol. 21, No. 4, (pp 384-393).

Noble, D. and Kirzl, J. (2203); "Objective Metrics for Evaluation of Collaborating Teams." Proceedings of the 2003 Command and Control Research Technology Symposium. Washington, D.C. National Defense University

Wegner, D.M. (1987) Transactive Memory: A Contemporary Analysis of Group Mind." In Theories of Group Behavior, eds. Brian Mullen and George R. Goethals, 185-206. New York: Springer-Verlag.

Zsambok, C. E., Klein, G., Kyne, M., and Klinger, D.W.(1993); Advanced Team Decision Making: A Model for High Performance Teams. Fairborn, OH: Klein Associates, Inc.